

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor : Masaaki TAKASE, et al.  
Filed : Concurrently herewith  
For : COMMON KEY ENCRYPTION.....  
Serial No. : Concurrently herewith

November 25, 2003

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**PRIORITY CLAIM AND**  
**SUBMISSION OF PRIORITY DOCUMENT**

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-348748** filed **November 29, 2002**, a certified copy of which is enclosed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "TJ Bean", written over a horizontal line.

Thomas J. Bean  
Reg. No. 44,528

Katten Muchin Zavis Rosenman  
575 Madison Avenue  
New York, NY 10022-2585  
(212) 940-8800  
Docket No.: FUJY 20.758

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 2 年 1 1 月 2 9 日  
Date of Application:

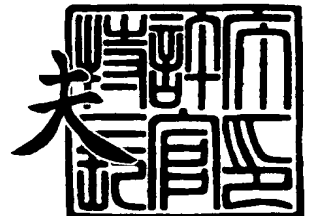
出 願 番 号            特 願 2 0 0 2 - 3 4 8 7 4 8  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 2 - 3 4 8 7 4 8 ]

出      願      人            富 士 通 株 式 会 社  
Applicant(s):

2 0 0 3 年   8 月   4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0253262

【提出日】 平成14年11月29日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/16

【発明の名称】 共通鍵暗号化通信システム

【請求項の数】 10

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号富士通株式会社内

    【氏名】 高瀬 正明

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号富士通株式会社内

    【氏名】 掛水 光明

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号富士通株式会社内

    【氏名】 五十嵐 洋一郎

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号富士通株式会社内

    【氏名】 谷口 浩之

【発明者】

    【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号富士通西日本コミュニケーション・システムズ株式会社内

    【氏名】 山村 新也

**【発明者】**

**【住所又は居所】** 福岡県福岡市早良区百道浜 2 丁目 2 番 1 号富士通西日本  
コミュニケーション・システムズ株式会社内

**【氏名】** 岩本 勝徳

**【発明者】**

**【住所又は居所】** 福岡県福岡市早良区百道浜 2 丁目 2 番 1 号富士通西日本  
コミュニケーション・システムズ株式会社内

**【氏名】** 小金丸 啓

**【発明者】**

**【住所又は居所】** 福岡県福岡市早良区百道浜 2 丁目 2 番 1 号富士通西日本  
コミュニケーション・システムズ株式会社内

**【氏名】** 若目田 宏

**【特許出願人】**

**【識別番号】** 000005223

**【氏名又は名称】** 富士通株式会社

**【代理人】**

**【識別番号】** 100089244

**【弁理士】**

**【氏名又は名称】** 遠山 勉

**【選任した代理人】**

**【識別番号】** 100090516

**【弁理士】**

**【氏名又は名称】** 松倉 秀実

**【連絡先】** 0 3 - 3 6 6 9 - 6 5 7 1

**【手数料の表示】**

**【予納台帳番号】** 012092

**【納付金額】** 21,000円

**【その他】**

国等の委託研究の成果に係る特許出願（平成 1 4 年度通  
信・放送機構「ヒューマンセントリック ユビキタスネ

ットワーク基盤システムに関する研究開発」委託研究、  
産業活力再生特別措置法第 3 0 条の適用を受けるもの)

**【提出物件の目録】**

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705606

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 共通鍵暗号化通信システム

【特許請求の範囲】

【請求項 1】 鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、

前記鍵送信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第 1 保持手段と、

送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第 1 設定手段と、

を備え、

前記鍵受信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第 2 保持手段と、

送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第 2 設定手段と、

を備える、共通鍵暗号化通信システム。

【請求項 2】 前記鍵送信装置は、暗号化鍵を取得する取得手段をさらに備え、

前記第 1 保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、

前記第 1 設定手段は、前記第 1 保持手段による更新後の保持鍵に基づいて、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、請求項 1 に記載の共通鍵暗号化通信システム。

【請求項 3】 前記鍵送信装置は、暗号化鍵を生成する生成手段を備え、

前記取得手段は、前記生成手段によって生成された暗号化鍵を取得する、請求項 2 に記載の共通鍵暗号化通信システム。

【請求項 4】 前記鍵送信装置は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する第 1 送信手段をさらに備える、請求項 2 に記載の共通鍵暗号化通信システム。

【請求項 5】 前記鍵受信装置は、前記鍵送信装置から送信される暗号化鍵を受信する第 2 受信手段をさらに備え、

前記第 2 受信手段が暗号化鍵を受信した場合、

前記第 2 保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記第 2 受信手段によって受信した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、

前記第 2 設定手段は、前記第 2 保持手段による更新号の保持鍵に基づいて、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、請求項 4 に記載の共通鍵暗号化通信システム。

【請求項 6】 前記鍵受信装置は、所定メッセージを鍵送信装置に対して送信する第 2 送信手段を備え、

前記鍵送信装置は、前記鍵受信装置から送信される所定メッセージを受信する第 1 受信手段を備える、請求項 1 に記載の共通鍵暗号化システム。

【請求項 7】 前記第 1 及び第 2 保持手段は、それぞれ初期化鍵を保持する、請求項 4 に記載の共通鍵暗号化通信システム。

【請求項 8】 鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵送信装置であって、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、

送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵送信装置。

【請求項 9】 鍵送信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵受信装置であって、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、

送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の

暗号化鍵を、それぞれ設定する設定手段とを備える、鍵受信装置。

【請求項 1 0】 鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う方法であって、

前記鍵送信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、

送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定し、

前記鍵受信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、

送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する、共通鍵暗号化通信方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は共通鍵を用いた暗号化方式を用いる場合の共通鍵の共有方法に関する。

【0 0 0 2】

【従来の技術】

ネットワークの発展に伴い、ネットワーク上を流れるトラフィックも多様化している。この中には他人に知られてはならない秘密情報等も含まれており、それを秘匿する手段としてIPsec等による暗号化通信技術が確立されている。

【0 0 0 3】

暗号化通信方式である VPN (Virtual Private Network) 特に、IPsec (IP security protocol) を利用した通信方式では、暗号化通信の開始前に通信対象の端末が相互に IKE (Internet Key Exchange) プロトコルを利用して暗号鍵を交換し、通信時にこれを用いてデータの暗号/復号化を行うことが規定されている。

【0 0 0 4】

上述の暗号鍵は、同一の鍵内容を長時間利用すると悪意ある傍受者に鍵内容を解読される恐れがあることから、個々の鍵には有効期限が設定されており、この



期限を越えて通信に利用することができない規定となっている。このため、IPsecによるVPN通信中の端末は、当該有効期限の満了前に再度鍵交換手順を実施して新規に暗号鍵を取得して定期的に更新することで、暗号通信の堅牢性を確保している。

#### 【0 0 0 5】

上述の一連の鍵交換機構では、各端末（通信のエンドポイント）が保持する暗号鍵は、現在通信中のものが満了する前に、次の鍵交換を実施し、この鍵交換が完了した時点で新たな鍵に切り替えて暗号化通信を継続することが可能である。

#### 【0 0 0 6】

上述の機構は一对一の通信においては問題がないと考えられるが、一サーバに対し多数のクライアントが暗号化通信を行う場合には、サーバの鍵交換による負荷が問題になると考えられる。これを解決するためには例えばサーバからクライアントに鍵を配布する方法が考えられるが、この方法において定期的に鍵を更新する場合、鍵配布中や鍵を配布するためのメッセージが破棄された場合に通信が途切れてしまうという問題があった。即ち、鍵配布時の鍵紛失時のリカバリー手順は考慮されておらずVPNをモバイル通信と併用する際の懸念事項となる。

#### 【0 0 0 7】

なお、インターネット等の標準的なプロトコルを利用しつつ、1つのセッション中における暗号化鍵の交換を可能として、通信データの機密性・秘蔵性を確保するものが知られている（例えば、特許文献1参照）。

#### 【0 0 0 8】

##### 【特許文献1】

特開 2 0 0 2 - 2 1 7 8 9 6 号公報

#### 【0 0 0 9】

##### 【発明が解決しようとする課題】

本発明の課題は、共通鍵暗号化通信を行う二つの装置の一方が他方に暗号化鍵を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も通信を継続するための技術を提供することにある。

#### 【0 0 1 0】

**【課題を解決するための手段】**

本発明は、上記課題を解決するために、鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第1保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第1設定手段と、を備え、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第2保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第2設定手段と、を備える構成とした。

**【0011】**

本発明によれば、鍵送信装置と鍵受信装置がそれぞれ、共通鍵として最新の暗号化鍵及び一世代前の二世代の暗号化鍵を保持するため、鍵送信装置が鍵受信装置に暗号化鍵等を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も通信を継続することが可能となる。なお、鍵送信装置としては、Mobile IPでのHAに限られない。例えば、インターネット上のサーバ等の情報処理端末であってもよい。また、鍵受信装置としては、Mobile IPでのMNに限られない。例えば、インターネット上のサーバ等と通信可能な情報処理端末であってもよい。

**【0012】**

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、暗号化鍵を取得する取得手段をさらに備え、前記第1保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第1設定手段は、前記第1保持手段による更新後の保持鍵に基づいて、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する。

**【0013】**

このようにすれば、鍵送信装置において暗号化鍵を更新することが可能となる。

## 【0014】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、暗号化鍵を生成する生成手段を備え、前記取得手段は、前記生成手段によって生成された暗号化鍵を取得する。

## 【0015】

このようにすれば、鍵送信装置は、自ら生成した鍵を取得することが可能となる。また、鍵送信装置は、外部の鍵生成部に鍵の生成を依頼してこの鍵を取得するようにしてもよいし、又は、自己又は外部が保持する鍵データベース等から鍵を読み出すようにしてもよい。

## 【0016】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する第1送信手段をさらに備える。この送信のタイミングとしては各種のものが考えられる。例えば、鍵受信装置から所定メッセージを受信した場合に送信するようにしてもよいし、自己でタイマを保持しておき、所定タイミングで送信するようにしてもよい。

## 【0017】

このようにすれば、一（鍵送信装置）対多（鍵受信装置）の共通鍵暗号化通信における、鍵の共有に要する負荷が低減される。

## 【0018】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、前記鍵送信装置から送信される暗号化鍵を受信する第2受信手段をさらに備え、前記第2受信手段が暗号化鍵を受信した場合、前記第2保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記第2受信手段によって受信した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第2設定手段は、前記第2保持手段による更新号の保持鍵に基づいて、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する。

## 【0019】

このようにすれば、鍵受信装置において暗号化鍵を更新することが可能となる。

#### 【 0 0 2 0 】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定メッセージを鍵送信装置に対して送信する第 2 送信手段を備え、前記鍵送信装置は、前記鍵受信装置から送信される所定メッセージを受信する第 1 受信手段を備える。

#### 【 0 0 2 1 】

このようにすれば、鍵送信装置は、所定メッセージの受信をきっかけとして、鍵の生成や鍵の配布等を行うことが可能となる。

#### 【 0 0 2 2 】

上記共通鍵暗号化通信システムにおいては、例えば、前記第 1 及び第 2 保持手段は、それぞれ初期化鍵を保持する。

#### 【 0 0 2 3 】

このようにすれば、鍵受信装置の起動時（二世代の鍵のいずれも設定されていない状態）や、鍵受信装置からの鍵更新要求に対する鍵送信装置からの応答が得られない場合（鍵送信装置の障害等により鍵送信装置の二世代鍵が失われていると考えられる状態）であっても、その初期化鍵による暗号化が可能となるため、暗号化通信を継続することが可能となる。

#### 【 0 0 2 4 】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵初期化要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵初期化要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第 1 保持手段は、共通の初期化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する。

#### 【 0 0 2 5 】

このようにすれば、鍵送信装置は、鍵受信装置からの初期化要求メッセージに応じて、自己の暗号化鍵を初期化することが可能となる。

**【 0 0 2 6 】**

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵更新要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵更新要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第 1 保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する。

**【 0 0 2 7 】**

このようにすれば、鍵送信装置は、鍵受信装置からの鍵更新要求メッセージに応じて、自己の暗号化鍵を更新することが可能となる。

**【 0 0 2 8 】**

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、鍵更新時期を決定するための手段を備え、前記第 2 送信手段は、鍵更新時期に達した場合に、鍵更新要求メッセージを鍵送信装置に対して送信する。

**【 0 0 2 9 】**

このようにすれば、鍵受信装置は、所定タイミングで（例えば周期的に）、鍵更新要求メッセージを送信することが可能となる。

**【 0 0 3 0 】**

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、鍵更新時期を決定するための手段を備え、第 1 送信手段は、鍵更新時期に達した場合に、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する。

**【 0 0 3 1 】**

このようにすれば、鍵送信装置は、鍵受信装置からの要求にかかわらず、自己の判断で、暗号化鍵を送信することが可能となる。

**【 0 0 3 2 】**

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵再送要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵再送要求メッセージを受信した場合、第 1 送信手段は、前記取得手段によって取得した暗号化鍵

を鍵受信装置に対して送信する。

【0 0 3 3】

このようにすれば、鍵送信装置は、鍵受信装置からの鍵再送要求メッセージに応じて、暗号化鍵を送信することが可能となる。

【0 0 3 4】

上記共通鍵暗号化通信システムにおいては、例えば、前記第 1 送信手段は、前記第 1 及び第 2 保持手段がいずれの鍵も保持していない状態で、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する。この場合、初期化鍵を用いて通信することになる。

【0 0 3 5】

本発明は、鍵送信装置として次のように特定できる。鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵送信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵送信装置。

【0 0 3 6】

なお、鍵送信装置としては、Mobile IPでのHAに限られない。例えば、インターネット上のサーバ等の情報処理端末であってもよい。

【0 0 3 7】

また、本発明は、鍵受信装置として次のように特定できる。鍵送信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵受信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵受信装置。

【0 0 3 8】

なお、鍵受信装置としては、Mobile IPでのMNに限られない。例えば、インターネット上のサーバ等と通信可能な情報処理端末であってもよい。

【0 0 3 9】

また、本発明は、方法の発明として次のように特定できる。鍵送信装置と鍵受

信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う方法であって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定し、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する、共通鍵暗号化通信方法。

#### 【0040】

##### 【発明の実施の形態】

以下、本発明の実施の形態である共通鍵暗号化通信システムについて図面を参照しながら説明する。図1は、共通鍵暗号化通信システムの概略構成を説明するための図である。

#### 【0041】

図1に示すように、共通鍵暗号化通信システムは、鍵送信装置と鍵受信装置とを備えており、両者間で、所定タイミングで更新される共通鍵による暗号化通信を行う。鍵の配布は鍵送信装置が行う。このため、一（鍵送信装置）対多（鍵受信装置）の共通鍵暗号化通信における、鍵の共有に要する負荷が低減される。

#### 【0042】

従来、鍵送信装置と鍵受信装置がそれぞれ受信鍵を一つだけを管理していたので、鍵送信側が鍵を生成して自らに設定した後、生成した鍵を含む鍵配布メッセージを鍵受信側が受信して設定するまでの間、鍵の不一致のため暗号化通信が不可能になる。これを解決するため、本実施形態の共通鍵暗号化通信システムでは、双方が受信用に鍵を二世代保持、管理し（N番目の鍵及びN-1番目の鍵）、鍵送信側の暗号化鍵（送信用）には一世代前の鍵（N-1番目の鍵）を設定し（用い）、鍵受信側の暗号化鍵（送信用）には最新の鍵（N番目の鍵）を設定する（用いる）。また、双方とも復号化鍵（受信用）として最新/一世代前（N番目の鍵及びN-1番目の鍵）の双方を設定し、どちらでも復号できるようにする。

#### 【0043】

本実施形態においては、鍵送信装置と鍵受信装置との間でM o b i l e I P

v 6 による通信を行うものとする。

【 0 0 4 4 】

まず、M o b i l e I P v 6 の概要について説明する。M o b i l e I P v 6 は、移動端末としてのMN (mobile node) が当初のネットワーク・セグメント (ホームネットワークという) とは異なるネットワーク・セグメントへ移動しても、同一の I P アドレスで通信を継続するための仕組みを提供する。そのために、当初のネットワーク・セグメントにルーター等のH A (home agent) が設けられている。

【 0 0 4 5 】

MN は、当初のネットワーク・セグメントとは異なるネットワーク・セグメントへ移動したことを検出すると、その移動先ネットワーク上のアドレス (一時的なcare-ofアドレス。気付アドレスともいう) を生成してH A に登録する。具体的には、MN は、登録要求 (B U : Binding Update) をH A に対して送信する。これにより、新しいcare-ofアドレス (送信元アドレスとして含まれている) をH A に知らせる。

【 0 0 4 6 】

H A は、MN からの登録要求 (B U) を受信すると、care-ofアドレスを登録する。これとともに、H A は、登録応答 (B A : binding acknowledgement) をその登録要求送信元のMN に対して送信する。以後、H A は、登録されているMN 宛のパケットを受け取った場合には、そのパケットをカプセル化し (care-ofアドレスが宛先アドレス) トンネリングにより移動先のネットワーク・セグメントへ転送する。これにより、MN は当初のネットワーク・セグメントとは異なるネットワーク・セグメントへ移動しても、同一の I P アドレスで通信を継続することが可能となっている。

【 0 0 4 7 】

次に、鍵送信装置及び鍵受信装置の構成について図面を参照しながら説明する。本実施形態においては、上記H A (home agent) が鍵送信装置 1 0 0 に、MN (mobile node) が鍵受信装置 2 0 0 に、それぞれ相当する。図 2 は、鍵送信装置 (H A) の構成例を説明するための図である。図 3 は、鍵受信装置 (MN) の構成



例を説明するための図である。

#### 【0048】

図2に示すように、鍵送信側装置(HA)100は、パケット送受信部101、鍵生成/管理部102、暗号化/復号化部103、及び、プロトコル制御部104等を備えている。また、SPI値を用いて鍵の更新/鍵の初期化を判断する場合は、SPI-鍵対応テーブルを鍵生成/管理部が保持する(図21参照)。

#### 【0049】

パケット送受信部101は、Mobile IPv6のネットワークに接続されており、鍵受信装置(MN)200等からの自己宛のパケット(例えば、所定メッセージを含むパケット)を受信したり、鍵受信装置(MN)200等宛のパケットをネットワークへ送出する。このパケット送受信部101により、鍵受信装置(MN)200からの所定メッセージ(鍵初期化要求メッセージ、鍵更新要求メッセージ、又は、鍵再送要求メッセージ等)を受信できるため、鍵受信装置(MN)200からの要求により、強制的に鍵更新を行うことが可能となる。また、更新した鍵を鍵受信装置(MN)200へ送信することが可能となる。

#### 【0050】

鍵生成/管理部102は、所定タイミングで暗号化鍵を生成(又は、外部の鍵生成部に暗号化鍵の生成を依頼してこれを取得、又は、自己又は外部が保持する鍵データベース等から暗号化鍵を読み出し)する。鍵生成/管理部102は、その生成等された暗号化鍵(最新の暗号化鍵)とその直前のタイミングで生成等された暗号化鍵(一世代前の暗号化鍵)、及び、予め設定されている初期化用鍵を保持、管理する。

#### 【0051】

これらの鍵は後述のように更新されるが、その場合でも、鍵生成/管理部102は、その更新(生成等)された暗号化鍵(最新の暗号化鍵)とその直前のタイミングで更新(生成等)された暗号化鍵(一世代前の暗号化鍵)、及び、予め設定(又は配布)されている初期化用鍵を保持、管理する。この鍵生成/管理部102により、一定周期又は鍵受信装置(MN)200から要求があった場合に動的に鍵を生成し、更新することが可能になる。

**【0052】**

また、この鍵生成／管理部 102 が受信用の鍵を二世代管理することにより、鍵受信装置 (MN) 200 が一世代前の鍵又は最新の鍵のどちらでパケットを暗号化しても、復号化することが可能となる。また、この鍵生成／管理部 102 が送信用の鍵を一つ管理、設定することにより、鍵送信装置 (HA) 100 は、一世代前の鍵でパケットを暗号化し、送信することが可能となる。

**【0053】**

また、この鍵生成／管理部 102 が初期化用の鍵を一つ管理、設定することにより、この鍵で暗号化された動的鍵初期化要求メッセージを復号化することができる。また、この鍵で暗号化されたことを鍵送信装置 (HA) 100 が認識することにより、動的鍵の初期化を行うことが可能となる。

**【0054】**

以下、N 回目の鍵の作成で作られた鍵を N 番目の鍵と呼ぶ。即ち、初回の鍵配布で鍵送信装置 (HA) 100 から鍵受信装置 (MN) 200 へ送信される鍵は、1 番目の鍵である。鍵生成／管理部 102 は、鍵受信装置 (MN) 200 ごと (MN が複数の場合) に二世代の鍵及び初期化用鍵を保持、管理する。鍵生成／管理部 102 は、通常、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する。

**【0055】**

暗号化／復号化部 103 は、鍵受信装置 (MN) 200 からの受信パケットが暗号化されている場合に、その受信パケットを受信用の暗号化鍵 (のいずれか) で復号化したり、鍵受信装置 (MN) 200 に対する送信パケットを送信用の暗号化鍵で暗号化するためのものである。暗号化／復号化部 103 は、その復号化又は暗号化の際には、鍵生成／鍵管理部 102 を参照して、適切な暗号化鍵を使用する。

**【0056】**

プロトコル制御部 104 は、暗号化／復号化部 103 により復号化された鍵受信装置 (MN) 200 からの受信パケットの内容を判定したり、鍵受信装置 (MN) 200 に対して送信する鍵配布メッセージを作成したりするためのものである。

る。

#### 【0057】

図3に示すように、鍵受信装置(MN)200は、パケット送受信部201、鍵管理部202、暗号化／復号化部203、及び、プロトコル制御部204等を備えている。

#### 【0058】

パケット送受信部201は、Mobile IPv6のネットワークに接続されており、鍵送信装置(HA)100等からの自己宛のパケットを受信したり、鍵送信装置(HA)100等宛のパケットをネットワークへ送出する。このパケット送受信部201が鍵配布メッセージを受信することにより、鍵送信装置(HA)100からの鍵の配布が可能となる。

#### 【0059】

鍵管理部202は、鍵送信装置(HA)100から配布される鍵配布メッセージに含まれる暗号化鍵(最新の鍵及び一世代前の暗号化鍵)、及び、予め設定されている初期化用鍵(いずれの鍵も鍵送信装置(HA)100と共通)を保持、管理する。

#### 【0060】

鍵管理部202は、通常、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する。これらの鍵は後述のように更新されるが、その場合でも、鍵管理部202は、その更新(生成等)された暗号化鍵(最新の暗号化鍵)とその直前のタイミングで更新(生成等)された暗号化鍵(一世代前の暗号化鍵)、及び、予め設定(又は配布)されている初期化用鍵を保持、管理する。

#### 【0061】

この鍵管理部202が受信用の鍵を二世代管理／設定することにより、鍵送信装置(HA)100が最新鍵又は一世代前の鍵のどちらでパケットを暗号化しても、復号化することが可能となる。また、この鍵管理部202が送信用の鍵を一つ管理／設定することにより、鍵受信装置(MN)200は最新の鍵でパケットを暗号化し、送信することが可能となる。

**【 0 0 6 2 】**

また、この鍵生成／管理部 1 0 2 が初期化用の鍵を一つ管理／設定することにより、動的鍵初期化要求メッセージも暗号化することができ、またこの鍵で暗号化されたことを鍵送信側装置が認識することによって初期化を行うことが可能となる。

**【 0 0 6 3 】**

暗号化／復号化部 2 0 3 は、鍵送信装置（H A） 1 0 0 からの受信パケットが暗号化されている場合に、その受信パケットを受信用の暗号化鍵（のいずれか）で復号化したり、鍵送信装置（H A） 1 0 0 に対する送信パケットを送信用の暗号化鍵で暗号化するためのものである。暗号化／復号化部 2 0 3 は、その復号化又は暗号化の際には、鍵管理部 2 0 2 を参照して、適切な暗号化鍵を使用する。

**【 0 0 6 4 】**

プロトコル制御部 2 0 4 は、暗号化／復号化部 2 0 3 により復号化された鍵送信装置（H A） 1 0 0 からの所定メッセージ（鍵初期化メッセージ、鍵更新メッセージ、鍵再送要求メッセージ等）を作成したりするためのものである。このプロトコル制御部 2 0 4 が鍵更新要求メッセージ又はこれに相当するメッセージを生成することにより、鍵受信側装置（M N） 2 0 0 の意向又は鍵配布メッセージがネットワーク上で破棄された場合に、鍵受信装置（M N） 2 0 0 が最新の鍵を要求することが可能になる。また、プロトコル制御部 2 0 4 が鍵初期化要求メッセージ又はこれに相当するメッセージを生成することにより、鍵受信装置（M N） 2 0 0 障害等で双方の鍵の初期化が必要となった場合に、鍵送信側装置にそれを要求することが可能となる。

**【 0 0 6 5 】**

次に、上記構成の共通鍵暗号化通信システムにおける暗号化通信の動作について図面を参照しながら説明する。

**【 0 0 6 6 】**

まず、鍵受信装置（M N） 2 0 0 からの所定メッセージにより、鍵送信装置（H A） 1 0 0 が暗号化鍵を更新、鍵受信装置（M N） 2 0 0 に対して配布する処理について説明する。ここでは、鍵受信装置（M N） 2 0 0 からの登録要求（B

U)とともに所定メッセージを送信し、鍵送信装置(HA)100からの登録応答(BA)とともに鍵配布メッセージを送信するものとする。

#### 【0067】

(1) 鍵受信装置(MN)200からの所定メッセージが鍵初期化メッセージである場合の動作例(その1)

#### 【0068】

図4は、鍵受信装置(MN)起動時に動的鍵(共通鍵)を配布する手順を説明するためのシーケンス図である。図5及び図7は、鍵受信装置(MN)に着目したシーケンス図である。図6は、鍵送信装置(HA)に着目したシーケンス図である。図17は、鍵送信装置(HA)における概略処理を説明するためのフローチャートである。図18は、鍵受信装置(MN)における概略処理を説明するためのフローチャートである。

#### 【0069】

ここでは、鍵受信装置(MN)200起動時には鍵受信装置(MN)200及び鍵送信装置(HA)100共に動的鍵(N番目の鍵、N-1番目の鍵)は保持(設定)されておらず、初期化鍵のみが双方に保持(設定)されているものとする。

#### 【0070】

鍵受信装置(MN)200は起動すると初期設定を行う。ここでは、暗号化鍵(送信用)及び復号化鍵(受信用)として共に初期化鍵が設定される。次に、図4、図5に示すように、鍵受信装置(MN)200は、鍵を初期化すべき事象が発生したとして(S100)、鍵初期化要求メッセージを含むBUを作成する。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部204は、拡張ヘッダ部分(又はペイロード部分)に鍵初期化要求メッセージ及びBUを設定(又は配置)したIPパケットを作成する(S101)。

#### 【0071】

このBU(IPパケット)は後述のように暗号化/復号化部203により暗号化されるので、その暗号化に用いた鍵を受信側(HA)で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部204は、そのBU(

IP パケット) に AH (authentication header) 又は ESP (encapsulating security payload) を適用する。なお、AH のみを適用した場合は、BA に含んで配布する鍵を別途暗号化 (AH で用いる鍵を流用することも可能) する必要がある。

#### 【0072】

AH 又は ESP には SPI (security parameters index) のフィールドが含まれるので、プロトコル制御部 204 は、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のように BU (IP パケット) は送信用の鍵 (初期化鍵) で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部 204 は、作成した BU (IP パケット) を暗号化/復号化部 203 へ渡す (S102)。

#### 【0073】

暗号化/復号化部 203 は、鍵管理部 202 を参照して (S103) (送信用の鍵 (初期化鍵) を用いて) プロトコル制御部 204 からの BU (IP パケット) を暗号化する (S104)。暗号化/復号化部 203 による暗号化は次のようにして行う。例えば、鍵初期化要求メッセージ及び BU が IP v6 の IP パケットの拡張ヘッダに配置されている場合には、暗号化/復号化部 203 は、IP ヘッダとデータ部とともに暗号化して、それに新たな IP ヘッダを付加する (トンネル・モード)。一方、鍵初期化要求メッセージ及び BU が IP パケットのペイロードに配置されている場合には、暗号化/復号化部 203 は、IP ヘッダ以外のデータ部を暗号化する (トランスポート・モード)。又は、IP ヘッダとデータ部とともに暗号化して、それに新たな IP ヘッダを付加する。暗号化/復号化部 203 は、暗号化した BU (IP パケット) をパケット送受信部 201 へ渡す (S105)。

#### 【0074】

パケット送受信部 201 は、暗号化/復号化部 203 からの BU (IP パケット) を鍵送信装置 (HA) 100 に対して送信する (S106)。

#### 【0075】



図6、図17に示すように、鍵送信装置(HA)100は、鍵受信装置(MN)200からのBU(鍵初期化要求メッセージを含むIPパケット)を受信する(S107)。パケット送受信部101は、その受信したパケットが暗号化されていれば暗号化／復号化部103へ渡す(S108)。暗号化／復号化部103は、受信したパケットのSPI値及び鍵生成／管理部102を参照し、そのSPI値によって指定される鍵(ここでは初期化鍵)でパケットを復号化し(S109)、登録要求(BU)の処理後、プロトコル制御部104へ渡す(S110)。

#### 【0076】

プロトコル制御部104は、暗号化／復号化部103からのパケットの内容を判定し(S111)、鍵初期化要求メッセージであればそれを鍵生成／管理部102に通知する(S112)。

#### 【0077】

鍵生成／管理部102は、新たな鍵を生成する(S113)(又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。)。鍵生成／管理部102は、鍵の設定を初期化する(S114)。

#### 【0078】

具体的には、暗号化鍵(送信用)として初期化鍵を、復号化鍵(受信用)として新たな鍵及び初期化鍵を、それぞれ設定する(図1参照)。そして、鍵生成／管理部102は、その鍵の設定後、その生成した新たな鍵をプロトコル制御部104に渡す(S115)。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

#### 【0079】

プロトコル制御部104は鍵配布メッセージを含む登録応答(BA)を作成する(S116)。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部104は、拡張ヘッダ部分(又はペイロード部分)に鍵配布メッセージ(新たな鍵を含む)及びBAを設定(又は配置)したBA(IP

パケット)を作成する。

#### 【0080】

このBA(IPパケット)は後述のように暗号化／復号化部103により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部104は、そのBA(IPパケット)にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能)する必要がある。

#### 【0081】

AH又はESPにはSPI(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにBA(IPパケット)は送信用の鍵(初期化鍵)で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部104は、作成したBA(IPパケット)を暗号化／復号化部103へ渡す(S117)。

#### 【0082】

暗号化／復号化部103は、鍵生成／管理部102を参照して(S118)(送信用の鍵(初期化鍵)を用いて)そのBA(IPパケット)を暗号化する(S119)。暗号化／復号化部による暗号化は次のようにして行う。例えば、鍵配布メッセージ及びBAがIPv6のIPパケットの拡張ヘッダに配置されている場合には、暗号化／復号化部は、IPヘッダとデータ部をともに暗号化して、それに新たなIPヘッダを付加する(トンネル・モード)。

#### 【0083】

一方、鍵配布メッセージ及びBAがIPパケットのペイロードに配置されている場合には、暗号化／復号化部は、IPヘッダ以外のデータ部を暗号化する(トランスポート・モード)。又は、IPヘッダとデータ部をともに暗号化して、それに新たなIPヘッダを付加する。暗号化／復号化部は、暗号化したBA(IPパケット)をパケット送受信部101へ渡す(S120)。

#### 【0084】



パケット送受信部101は、暗号化／復号化部103からのBA（IPパケット）を鍵受信装置（MN）200に対して送信する（S121）。

#### 【0085】

図7、図18に示すように、鍵受信装置（MN）200は、鍵送信装置（HA）100からのBA（IPパケット）を受信する（S122）。パケット送受信部201は、受信したパケットが暗号化されていれば暗号化／復号化部203へ渡す（S123）。暗号化／復号化部203は、受信したパケットのSPI値及び鍵管理部202を参照し（S124）、そのSPI値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（S125）、プロトコル制御部204へ渡す（S126）。

#### 【0086】

プロトコル制御部204は暗号化／復号化部203からのパケットの内容を判定し（S127）、鍵配布メッセージであれば鍵（HAで生成された新たな鍵）を抽出し、その抽出した鍵を鍵管理部202に渡す（S128）。

#### 【0087】

鍵管理部202は、復号化鍵（受信用）として新たに（初期化鍵に加えて）その抽出した新たな鍵を設定する（S129）。また、鍵管理部は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する（初期化鍵そのものは削除されない）。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

#### 【0088】

（2）鍵受信装置（MN）200からの所定メッセージが鍵初期化メッセージである場合の動作例（その2）

#### 【0089】

図4は、鍵受信装置（MN）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図5及び図7は、鍵受信装置（MN）に着目したシーケンス図である。図6は、鍵送信装置（HA）に着目したシーケンス図である。図17は、鍵送信装置（HA）における概略処理を説明するためのフロー

チャートである。図18は、鍵受信装置(MN)における概略処理を説明するためのフローチャートである。

#### 【0090】

ここでは、鍵送信装置(HA)100、鍵受信装置(MN)200それぞれは、最新の鍵(N番目の鍵)及び一世代前の鍵(N-1番目の鍵)を保持、管理している(図1参照)。そして、鍵送信装置(HA)100の暗号化鍵(送信用)として一世代前の鍵(N-1番目の鍵)が、鍵受信装置(MN)の暗号化鍵(送信用)として最新の鍵(N番目の鍵)が、それぞれ使用可能であるように設定されている。また、鍵送信装置(HA)100、鍵受信装置(MN)200双方の復号化鍵(受信用)として、最新の鍵(N番目の鍵)、一世代前の鍵(N-1番目の鍵)の二つが使用可能であるように設定されている(図1参照)。

#### 【0091】

鍵受信装置(MN)200の要求による鍵の初期化には、鍵受信装置(MN)200の再起動時等がある。図4、図5に示すように、鍵受信装置(MN)200は、鍵受信装置(MN)200内部で鍵の初期化を決定した場合(S100)、鍵初期化要求メッセージを作成する。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部204は、拡張ヘッダ部分(又はペイロード部分)に鍵初期化要求メッセージ及びBUを設定(又は配置)したIPパケットを作成する(S101)。

#### 【0092】

このBU(IPパケット)は後述のように暗号化/復号化部203により暗号化されるので、その暗号化に用いた鍵を受信側(HA)で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部204は、そのBU(IPパケット)にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能)する必要がある。

#### 【0093】

AH又はESPにはSPI(security parameters index)のフィールドが含ま

れるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにIPパケットは送信用の鍵（N番目の鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてN番目の鍵を指定するデータが設定される。プロトコル制御部204は、作成したBU（鍵初期化要求メッセージを含むIPパケット）を暗号化／復号化部203へ渡す（S102）。

#### 【0094】

暗号化／復号化部203は、鍵管理部202を参照して（S103）（送信用の鍵（N番目の鍵）を用いて）プロトコル制御部204からのBU（IPパケット）を暗号化する（S104）。この暗号化の方法についてはすでに述べた。暗号化／復号化部203は、暗号化したBU（IPパケット）をパケット送受信部201へ渡す（S105）。

#### 【0095】

パケット送受信部201は、暗号化／復号化部203からのBU（IPパケット）を鍵送信装置（HA）100に対して送信する（S106）。

#### 【0096】

図6、図17に示すように、鍵送信装置（HA）100は、鍵受信装置（MN）200からのBU（鍵初期化要求メッセージを含むIPパケット）を受信し（S107）、鍵の生成と設定の初期化を行う。

#### 【0097】

具体的には、パケット送受信部101は、その受信したパケットが暗号化されていれば暗号化／復号化部103に渡す（S108）。暗号化／復号化部103は、受信したパケットのSPI値及び鍵生成/管理部102を参照し、そのSPI値によって指定される鍵（ここではN番目の鍵）でパケットを復号し（S109）、登録要求（BU）の処理後、プロトコル制御部104に渡す（S110）。

#### 【0098】

プロトコル制御部104は、暗号化／復号化部103からのパケットの内容を判定し（S111）、鍵初期化要求メッセージであればそれを鍵生成/管理部1

02に通知する(S112)。

#### 【0099】

鍵生成/管理部102は、新たな鍵(N+1番目の鍵)を生成する(S113) (又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。)。鍵生成/管理部102は、鍵の設定を初期化する(S114)。具体的には、鍵生成/管理部102は、復号化鍵(受信用)として新たにN+1番目の鍵と初期化鍵を設定し、N-1番目の鍵を削除する。

#### 【0100】

また、鍵生成/管理部102は、暗号化鍵(送信用)として新たに初期化鍵を設定し、N-1番目の鍵を削除する。なお、初期化鍵をN-1番目の鍵として扱い、次の鍵更新時には初期化鍵を削除する。そして、鍵生成/管理部102は、鍵の設定を更新後、その作成した新たな鍵(N+1番目の鍵)をプロトコル制御部104に渡す(S115)。

#### 【0101】

プロトコル制御部104は鍵配布メッセージを含む登録応答(BA)を作成する(S116)。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部104は、拡張ヘッダ部分(又はペイロード部分)に鍵配布メッセージ(新たな鍵を含む)及びBAを設定(又は配置)したBA(IPパケット)を作成する。

#### 【0102】

このBA(IPパケット)は後述のように暗号化/復号化部103により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部104は、そのBA(IPパケット)にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能)する必要がある。AH又はESPにはSPI(security parameters index)のフィールドが含まれるので

、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

#### 【0103】

ここでは、後述のようにIPパケットは送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部104は、作成したBA（IPパケット）を暗号化／復号化部103へ渡す（S117）。

#### 【0104】

暗号化／復号化部103は、鍵生成／管理部102を参照して（S118）（送信用の鍵（初期化鍵）を用いて）そのBA（IPパケット）を暗号化する（S119）。この暗号化の方法についてはすでに述べた。暗号化／復号化部103は、暗号化したIPパケットをパケット送受信部101へ渡す（S120）。

#### 【0105】

パケット送受信部101は、暗号化／復号化部103からのIPパケットを鍵受信装置（MN）200に対して送信する（S121）。

#### 【0106】

図7、図18に示すように、鍵受信装置（MN）200は、鍵送信装置（HA）100からのBA（鍵配布メッセージが付加されたIPパケット）を受信する（S122）。パケット送受信部201は、受信したパケットが暗号化されていれば暗号化／復号化部203へ渡す（S123）。暗号化／復号化部203は、受信したパケットのSPI値及び鍵管理部202を参照し（S124）、そのSPI値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（S125）、プロトコル制御部204へ渡す（S126）。

#### 【0107】

プロトコル制御部204は暗号化／復号化部203からのパケットの内容を判定し（S127）、鍵配布メッセージであれば鍵（HAで生成された新たなN+1番目の鍵）を抽出し、その抽出した鍵を鍵管理部202に渡す（S128）。

#### 【0108】

鍵管理部202は、復号化鍵（受信用）として新たに（初期化鍵に加えて）その抽出した新たな鍵を設定する（S129）。また、鍵管理部202は、暗号化

鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する（初期化鍵そのものは削除されない）。

#### 【0109】

（3）鍵受信装置（MN）200からの所定メッセージが鍵更新要求メッセージである場合の動作例

#### 【0110】

図8は、鍵受信装置（MN）からの鍵更新要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図9及び図7は、鍵受信装置（MN）に着目したシーケンス図である。図10は、鍵送信装置（HA）に着目したシーケンス図である。図17は、鍵送信装置（HA）における概略処理を説明するためのフローチャートである。図18及び図20は、鍵受信装置（MN）における概略処理を説明するためのフローチャートである。

#### 【0111】

ここでは、鍵送信装置（HA）100、鍵受信装置（MN）200それぞれは、最新の鍵（N番目の鍵）及び一世代前の鍵（N-1番目の鍵）を保持、管理している（図1参照）。そして、鍵送信装置（HA）100の暗号化鍵（送信用）として一世代前の鍵（N-1番目の鍵）が、鍵受信装置（MN）の暗号化鍵（送信用）として最新の鍵（N番目の鍵）が、それぞれ使用可能であるように設定されている。

#### 【0112】

また、鍵送信装置（HA）100、鍵受信装置（MN）200双方の復号化鍵（受信用）として、最新の鍵（N番目の鍵）、一世代前の鍵（N-1番目の鍵）の二つが使用可能であるように設定されている（図1参照）。また、鍵送信装置（HA）100でN+1番目の鍵が生成され、その鍵が鍵受信装置（MN）200に配布されるものとする（図8、図9参照）。

#### 【0113】

本例では、鍵受信装置（MN）200が鍵の更新を判断するため、鍵受信装置（MN）200の鍵管理部201に鍵更新タイマが内蔵されているものとし、鍵配布メッセージはMobile IPv6のBAメッセージと共に送信されるも

のとする。この鍵更新タイマにより、自らの鍵更新ポリシーに従って、鍵更新要求メッセージを送信することが可能となる。

#### 【0114】

図8、図9、図20に示すように、鍵受信装置(MN)200は、鍵受信装置(MN)200内部で鍵の更新を決定した場合(S200)(ここでは鍵管理部201において鍵更新タイマが満了した場合)、鍵更新要求メッセージを作成する。鍵管理部201において鍵更新タイマが満了すると、そのことをプロトコル制御部204に通知する(S201)。

#### 【0115】

これによりプロトコル制御部204は、BU送信を検知する(S202)。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部204は、拡張ヘッダ部分(又はペイロード部分)に鍵更新要求メッセージ及びBUを設定(又は配置)したIPパケットを作成する(S203)。

#### 【0116】

このBU(IPパケット)は後述のように暗号化/復号化部203により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部204は、そのBU(IPパケット)にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能)する必要がある。

#### 【0117】

AH又はESPにはSPI(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにIPパケットは送信用の鍵(N番目の鍵)で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてN番目の鍵を指定するデータが設定される。プロトコル制御部204は、作成したBU(鍵更新要求メッセージを含むIPパケット)を暗号化/復号化部203へ渡す(S204)。

#### 【0118】

暗号化／復号化部 203 は、鍵管理部 202 を参照して (S205) (送信用の鍵 (N 番目の鍵) を用いて) プロトコル制御部 204 からの BU (IP パケット) を暗号化する (S206)。この暗号化の方法についてはすでに述べた。暗号化／復号化部 203 は、暗号化した BU (IP パケット) をパケット送受信部 201 へ渡す (S207)。

#### 【0119】

パケット送受信部 201 は、暗号化／復号化部 203 からの BU (IP パケット) を鍵送信装置 (HA) 100 に対して送信する (S208)。

#### 【0120】

図 10、図 17 に示すように、鍵送信装置 (HA) 100 は、鍵受信装置 (MN) 200 からの BU (鍵更新要求メッセージを含む IP パケット) を受信し (S209)、鍵の生成と更新を行う。

#### 【0121】

具体的には、パケット送受信部 101 は、その受信したパケットが暗号化されていれば暗号化／復号化部 103 に渡す (S210)。暗号化／復号化部 103 は、受信したパケットの SPI 値及び鍵生成／管理部 102 を参照し (S211)、その SPI 値によって指定される鍵 (ここでは N 番目の鍵) でパケットを復号し (S212)、登録要求 (BU) の処理後、プロトコル制御部 104 に渡す (S213)。

#### 【0122】

プロトコル制御部 104 は、暗号化／復号化部 103 からのパケットの内容を判定し (S214)、鍵更新要求メッセージであればそれを鍵生成／管理部 102 に通知する (S215)。

#### 【0123】

鍵生成／管理部 102 は、新たな鍵 (N+1 番目の鍵) を生成する (S216) (又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。)。鍵生成／管理部 102 は、鍵の設定をする (S217)。具体的には、復号化鍵 (受信用) として新たに N+1 番



目の鍵を設定し、 $N-1$ 番目の鍵を削除する。また、暗号化鍵(送信用)として新たに $N$ 番目の鍵を設定し、 $N-1$ 番目の鍵を削除する。そして、鍵生成/管理部102は、その鍵の設定を更新後、その生成した新たな鍵( $N+1$ 番目の鍵)をプロトコル制御部104に渡す(S218)。

#### 【0124】

プロトコル制御部104は鍵配布メッセージを含む登録応答(BA)を作成する(S219)。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部104は、拡張ヘッダ部分(又はペイロード部分)に鍵配布メッセージ(新たな鍵を含む)及びBAを設定(又は配置)したBA(IPパケット)を作成する。

#### 【0125】

このIPパケットは後述のように暗号化/復号化部103により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部104は、そのBA(IPパケット)にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能)する必要がある。AH又はESPにはSPI(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

#### 【0126】

ここでは、後述のようにIPパケットは送信用の鍵( $N-1$ 番目の鍵)で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして $N-1$ 番目の鍵を指定するデータが設定される。プロトコル制御部104は、作成したBA(IPパケット)を暗号化/復号化部103へ渡す(S220)。

#### 【0127】

暗号化/復号化部103は、鍵生成/管理部102を参照して(S221)(送信用の鍵( $N-1$ 番目の鍵)を用いて)そのBA(IPパケット)を暗号化する(S222)。この暗号化の方法についてはすでに述べた。暗号化/復号化部103は、暗号化したIPパケットをパケット送受信部101へ渡す(S223)

）。

#### 【0128】

パケット送受信部101は、暗号化／復号化部103からのIPパケット（鍵配布メッセージを含むIPパケット）を鍵受信装置（MN）に対して送信する（S224）。

#### 【0129】

図7、図18に示すように、鍵受信装置（MN）200は、鍵送信装置（HA）100からのBA（鍵配布メッセージが付加されたIPパケット）を受信する（S122）。鍵受信装置（MN）200はそのIPパケット中に含まれる鍵を暗号化鍵（送信用）／復号化鍵（受信用）に設定する（S129）。

#### 【0130】

具体的には、パケット送受信部201は、受信したパケットが暗号化されていれば暗号化／復号化部203へ渡す（S123）。暗号化／復号化部203は、受信したパケットのSPI値及び鍵管理部202を参照し（S124）、そのSPI値によって指定される鍵（ここではN-1番目の鍵）でパケットを復号化し（S125）、プロトコル制御部204へ渡す（S126）。

#### 【0131】

プロトコル制御部204は暗号化／復号化部203からのパケットの内容を判定し（S127）、鍵配布メッセージであれば鍵（HAで生成された新たなN+1番目の鍵）を抽出し、その抽出した鍵を鍵管理部202に渡す（S128）。

#### 【0132】

鍵管理部202は、復号化鍵（受信用）として新たにその抽出した新たな鍵を設定する（S129）。また、鍵管理部202は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた鍵を削除する。

#### （4）鍵配布メッセージが破棄された場合のMNの動作例

#### 【0133】

図11は、鍵受信装置（MN）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図12及び図7

は、鍵受信装置 (MN) に着目したシーケンス図である。図 13 は、鍵送信装置 (HA) に着目したシーケンス図である。図 17 は、鍵送信装置 (HA) における概略処理を説明するためのフローチャートである。図 18 は、鍵受信装置 (MN) における概略処理を説明するためのフローチャートである。

#### 【0134】

ここでは、上記 (3) 鍵受信装置 (MN) 200 からの所定メッセージが鍵更新要求メッセージである場合の動作例において、鍵送信装置 (HA) 100 からの鍵配布メッセージ (N+1 番目の鍵を含む) を含む BA (IP パケット) が、鍵受信装置 (MN) 200 に到達せずに、途中で破棄されたものとする (図 11、図 12、図 13 参照)。この場合、鍵送信側装置 (HA) 100 のみ動的に更新される鍵が更新された状態となる (図 16 参照)。

#### 【0135】

図 11、図 12 に示すように、鍵受信装置 (MN) 200 は、鍵送信装置 (HA) 100 に対して送信した BU (IP パケット) に対する BA (IP パケット) を受信しないこと (例えば BU 送信後の一定期間内に BA を受信しないこと) を感知すると (S300)、再送のための BU (鍵再送要求メッセージを含む IP パケット) を上記鍵更新要求メッセージ等と同様にプロトコル制御部 204 によって作成し (S301)、これを暗号化／復号化部 203 へ渡す (S302)。

#### 【0136】

暗号化／復号化部 203 は、鍵管理部 202 を参照して (S303) (送信用の鍵 (N 番目の鍵) を用いて) プロトコル制御部 204 からの BU (IP パケット) を暗号化する (S304)。この暗号化の方法についてはすでに述べた。暗号化／復号化部 203 は、暗号化した BU (IP パケット) をパケット送受信部 201 へ渡す (S305)。

#### 【0137】

パケット送受信部 201 は、暗号化／復号化部 203 からの BU (IP パケット) を鍵送信装置 (HA) 100 に対して送信する (S306)。

#### 【0138】

図13、図17に示すように、鍵送信装置(HA)100は、鍵受信装置(MN)200からのBU(鍵再送要求メッセージを含むIPパケット)を受信し(S307)、鍵の再送を行う。

#### 【0139】

具体的には、パケット送受信部101は、その受信したパケットが暗号化されていれば暗号化／復号化部103に渡す(S308)。暗号化／復号化部103は、受信したパケットのSPI値及び鍵生成／管理部102を参照し(S309)、そのSPI値によって指定される鍵(ここではN番目の鍵)でパケットを復号し(S310)、登録要求(BU)の処理後、プロトコル制御部104に渡す(S311)。

#### 【0140】

プロトコル制御部104は、暗号化／復号化部103からのパケットの内容を判定し(S312)、鍵再送要求メッセージであればそれを鍵生成／管理部102に通知する(S313)。

#### 【0141】

鍵生成／管理部102は、新たな鍵を生成すること無く、前回配布して途中で破棄された最新の鍵(N+1番目の鍵)をプロトコル制御部104に渡す(S314)。

#### 【0142】

プロトコル制御部104は鍵配布メッセージを上記と同様に作成する(S315)。プロトコル制御部104は、作成したBA(IPパケット)を暗号化／復号化部103へ渡す(S316)。

#### 【0143】

暗号化／復号化部103は、鍵生成／管理部102を参照して(S317)(送信用の鍵(N番目の鍵)を用いて)そのBA(IPパケット)を暗号化する(S318)。この暗号化の方法についてはすでに述べた。暗号化／復号化部102は、暗号化したBA(IPパケット)をパケット送受信部101へ渡す(S319)。

#### 【0144】

パケット送受信部 101 は、暗号化／復号化部からの BA (IP パケット) を鍵受信装置 (MN) 200 に対して送信する (S320)。

#### 【0145】

図 7、図 18 に示すように、鍵受信装置 (MN) 200 は、鍵送信装置 (HA) 100 からの BA (鍵配布メッセージが付加された IP パケット) を受信する (S122)。鍵受信装置 (MN) 200 は、上記と同様にその IP パケット中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する (S123～S129)。

以上述べたように、本動作例では、鍵送信側装置 (HA) 100 は一世代前の動的鍵を暗号化鍵 (送信用) として使用することにより、動的鍵配布メッセージ (鍵配布メッセージともいう) が破棄されても通信が可能となる。

#### 【0146】

(5) 鍵送信側装置 (HA) の障害時等の鍵初期化手順

#### 【0147】

鍵送信装置 (HA) 100 の障害時等の鍵の初期化手順は以下である。ここでは、上記 (3) 鍵受信装置 (MN) 200 からの所定メッセージが鍵更新要求メッセージである場合の動作例において、鍵送信装置 (HA) 100 の障害等により鍵送信装置 (HA) の動的に更新される鍵 (N 番目の鍵及び N-1 番目の鍵) はすべて失われ、初期化用鍵のみが設定されているものとする。

#### 【0148】

鍵受信装置 (MN) 100 は、鍵送信装置 (HA) 100 に対して送信した BU (鍵更新要求メッセージを含む IP パケット) に対する BA (IP パケット) を一定期間後も受信しないことを検知すると、鍵送信装置 (HA) 100 の障害等が考えられるため、BU (鍵更新要求メッセージを含む IP パケット) を再送する。

#### 【0149】

鍵受信装置 (MN) 200 は、その再送した BU (IP パケット) に対する BA を一定期間後も受信しないことを検知すると、動的に更新される鍵の設定を初期化し、鍵初期化要求メッセージを含む BU を図 5 に示すように生成して (S1

01～S105) 鍵送信装置(HA) 100に送信する(S106)。

#### 【0150】

鍵送信装置(HA) 100は、図6及び図17に示すように、鍵受信装置(MN)からのBUに鍵初期化要求が含まれることを検知すると(S107～S111)、上記と同様に、鍵初期化メッセージ受信時の処理を行い(S113～S115)、BAに最新の鍵を含んだ鍵配布メッセージを付加し(S116)、鍵受信装置(MN)に送信する(S117～S121)。

#### 【0151】

図7、図18に示すように、鍵受信装置(MN)は、鍵配布メッセージが付加されたBAを受信すると(S122)、その中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する(S123～S129)。これについてはすでに述べたものと同様である。

#### 【0152】

以上述べたように、本動作例によれば、鍵受信装置(MN) 200が鍵更新要求メッセージ又はそれに相当するメッセージを再送することにより、正常な状態(最新の鍵が鍵受信装置(MN) 200の送受信用に設定された状態)に復帰することが可能となる。また、鍵更新要求メッセージを再送してもその返答として鍵配布メッセージが鍵受信装置に届かない場合、鍵受信装置(MN) 200は鍵初期化要求メッセージを鍵送信装置(HA) 100に送信することによって、初期化を行う。

#### 【0153】

以上述べたように、本動作例では、鍵受信側装置の障害等で鍵受信側装置と鍵送信側装置の動的鍵の不一致が起きた場合、動的鍵初期化メッセージ又はそれに相当するメッセージを鍵受信側装置が送信することにより、双方の動的鍵を初期化することが可能となる。

#### 【0154】

(6) 鍵送信側装置(HA)が鍵の更新を判断する場合のHAの動作例

#### 【0155】

図14は、鍵送信側装置(HA)が鍵の更新を判断して、動的鍵(共通鍵)を配

布する手順を説明するためのシーケンス図である。図7は、鍵受信装置(MN)に着目したシーケンス図である。図15は、鍵送信装置(HA)に着目したシーケンス図である。図18は、鍵受信装置(MN)における概略処理を説明するためのフローチャートである。図19は、鍵送信装置(HA)における概略処理を説明するためのフローチャートである。

#### 【0156】

ここでは、鍵送信装置(HA)100が鍵の更新(タイミング)を判断するため、鍵送信装置(HA)100の鍵生成/管理部102に鍵更新タイマが内蔵されているものとし、鍵配布メッセージはMobile IPv6のBAメッセージと共に送信されるものとする。この鍵更新タイマにより、一定周期で鍵の更新を行うことが可能となる。また、鍵送信装置(HA)100はN-1番目の鍵とN番目の鍵を保持しているとし、鍵送信装置(HA)100でN+1番目の鍵が生成され、その鍵が鍵受信装置(MN)200に配布されるものとする。

#### 【0157】

図14、図15に示すように、鍵生成/管理部102において鍵送信装置(HA)100の鍵更新タイマが満了すると(S400)、そのことをプロトコル制御部104に通知し(S401)、プロトコル制御部104はそれを鍵受信装置(MN)200ごとに保持する。例えば、プロトコル制御部104は、該当する鍵受信装置(MN)200に対する鍵更新タイマ満了フラグをオンにセットする(S412)。

#### 【0158】

鍵送信装置(HA)100は、鍵受信装置(MN)200からのBU(これには所定メッセージは含まれていない)を受信すると、BU処理を実行するとともに(S402)、プロトコル制御部104を参照して、そのBU送信元の鍵受信装置(MN)200の鍵更新タイマが満了したか否かを判定する。該当する鍵更新タイマが満了していれば(例えば該当する鍵受信装置(MN)200に対する鍵更新タイマ満了フラグがオンにセットされていれば)、プロトコル制御部104は、BAを作成する際、鍵生成/管理部102に鍵の更新を要求する。

#### 【0159】

鍵生成/管理部 102 は、新たな鍵 ( $N+1$  番目の鍵) を生成する (S403) (又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこれを取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。)。鍵生成/管理部 102 は、鍵の設定を更新する (S404)。具体的には、復号化鍵(受信用)として新たに  $N+1$  番目の鍵を設定し、 $N-1$  番目の鍵を削除する。また、暗号化鍵(送信用)として新たに  $N$  番目の鍵を設定し、 $N-1$  番目の鍵を削除する。そして、鍵生成/管理部 102 は、その鍵の設定を更新後、その生成した新たな鍵 ( $N+1$  番目の鍵) をプロトコル制御部 104 に渡す (S405)。

#### 【0160】

プロトコル制御部 104 は鍵配布メッセージを含む登録応答 (BA) を作成する (S406)。本実施形態では Mobile IPv6 を用いているので、例えば、プロトコル制御部 104 は、拡張ヘッダ部分 (又はペイロード部分) に鍵配布メッセージ (新たな鍵を含む) 及び BA を設定 (又は配置) した BA (IP パケット) を作成する。

#### 【0161】

この BA (IP パケット) は後述のように暗号化/復号化部 103 により暗号化されるので、その暗号化に用いた鍵を受信側 (MN) で知ることができるように (即ち受信側で復号できるように)、プロトコル制御部 104 は、その BA (IP パケット) に AH (authentication header) 又は ESP (encapsulating security payload) を適用する。なお、AH のみを適用した場合は、BA に含んで配布する鍵を別途暗号化 (AH で用いる鍵を流用することも可能) する必要がある。

#### 【0162】

AH 又は ESP には SPI (security parameters index) のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のように IP パケットは送信用の鍵 ( $N-1$  番目の鍵) で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして  $N-1$  番目の鍵を指定するデータが設定される。プロトコル制御部 104 は、作成し



たBA (IPパケット) を暗号化／復号化部103へ渡す (S407)。

#### 【0163】

暗号化／復号化部103は、鍵生成／管理部102を参照して (S408) (送信用の鍵 (N-1番目の鍵) を用いて) そのBA (IPパケット) を暗号化する (S409)。この暗号化の方法についてはすでに述べた。暗号化／復号化部103は、暗号化したIPパケットをパケット送受信部101へ渡す (S410)。

#### 【0164】

パケット送受信部101は、暗号化／復号化部103からのIPパケット (鍵配布メッセージを含むIPパケット) を鍵受信装置 (MN) に対して送信する (S411)。なお、BAの送信が完了すると、該当する鍵受信装置 (MN) 200に対する鍵更新タイマ満了フラグはオフにセットされる。

#### 【0165】

図7、図18に示すように、鍵受信装置 (MN) 200は、鍵送信装置 (HA) 100からのBA (鍵配布メッセージが付加されたIPパケット) を受信する (S122)。鍵受信装置 (MN) 200はそのIPパケット中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する (S129)。

#### 【0166】

具体的には、パケット送受信部201は、受信したパケットが暗号化されていれば暗号化／復号化部203へ渡す (S123)。暗号化／復号化部203は、受信したパケットのSPI値及び鍵管理部202を参照し (S124)、そのSPI値によって指定される鍵 (ここではN-1番目の鍵) でパケットを復号化し (S125)、プロトコル制御部204へ渡す (S126)。

#### 【0167】

プロトコル制御部204は暗号化／復号化部203からのパケットの内容を判定し (S127)、鍵配布メッセージであれば鍵 (HAで生成された新たなN+1番目の鍵) を抽出し、その抽出した鍵を鍵管理部202に渡す (S128)。

#### 【0168】

鍵管理部202は、復号化鍵 (受信用) として新たにその抽出した新たな鍵を

設定する（S129）。また、鍵管理部202は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた鍵を削除する。

#### 【0169】

次に、他の実施形態について説明する。

#### 【0170】

ここでは、IPsecによる暗号化通信を行っており、上記の実施形態とは異なり所定メッセージを用いることなく、そのSPI値により鍵の初期化/鍵の更新を判断する。鍵送信装置（HA）100は、鍵-SPI対応テーブル（図21参照）を保持しており、鍵受信装置（MN）200からのBU（所定メッセージを含まないIPパケット）に含まれるSPI値とそのテーブルを照合することで、受信パケットがどの鍵で暗号化されたのかを判定する。他の構成については、上記実施形態と同様であるので、その説明は省略する。

#### 【0171】

（7）鍵受信装置（MN）200からのBUが初期化鍵で暗号化されている場合の動作例（その1）

#### 【0172】

図22は、鍵受信装置（MN）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図5及び図7は、鍵受信装置（MN）に着目したシーケンス図である。図23は、鍵送信装置（HA）に着目したシーケンス図である。図28は、鍵送信装置（HA）における概略処理を説明するためのフローチャートである。

#### 【0173】

ここでは、鍵受信装置（MN）200起動時には鍵受信装置（MN）200及び鍵送信装置（HA）100共に動的鍵（N番目の鍵、N-1番目の鍵）は保持（設定）されておらず、初期化鍵のみが双方に保持（設定）されているものとする。

#### 【0174】

鍵受信装置（MN）200は起動すると初期設定を行う。ここでは、暗号化鍵

(送信用)及び復号化鍵(受信用)として共に初期化鍵が設定される。次に、図 2 2、図 5 に示すように、鍵受信装置 (MN) 2 0 0 は、鍵を初期化すべき事象が発生したとして (S 5 0 0)、BU を作成する。ここでは、上記実施形態と異なり、BU に鍵初期化要求メッセージを含まない。本実施形態では Mobile IP v 6 を用いているので、例えば、プロトコル制御部 2 0 4 は、拡張ヘッダ部分 (又はペイロード部分) に BU を設定 (又は配置) した IP パケットを作成する (S 5 0 1)。

#### 【0 1 7 5】

この BU (IP パケット) は後述のように暗号化／復号化部 2 0 3 により暗号化されるので、その暗号化に用いた鍵を受信側 (HA) で知ることができるように (即ち受信側で復号できるように)、プロトコル制御部 2 0 4 は、その BU (IP パケット) に AH (authentication header) 又は ESP (encapsulating security payload) を適用する。なお、AH のみを適用した場合は、BA に含んで配布する鍵を別途暗号化 (AH で用いる鍵を流用することも可能) する必要がある。

#### 【0 1 7 6】

AH 又は ESP には SPI (security parameters index) のフィールドが含まれるので、プロトコル制御部 2 0 4 は、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のように BU (IP パケット) は送信用の鍵 (初期化鍵) で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部 2 0 4 は、作成した BU (IP パケット) を暗号化／復号化部 2 0 3 へ渡す (S 5 0 2)。

#### 【0 1 7 7】

暗号化／復号化部 2 0 3 は、鍵管理部 2 0 2 を参照して (S 5 0 3) (送信用の鍵 (初期化鍵) を用いて) プロトコル制御部 2 0 4 からの BU (IP パケット) を暗号化する (S 5 0 4)。暗号化／復号化部 2 0 3 による暗号化は次のようにして行う。

#### 【0 1 7 8】

例えば、鍵初期化要求メッセージ及びBUがIPv6のIPパケットの拡張ヘッダに配置されている場合には、暗号化／復号化部203は、IPヘッダとデータ部をともに暗号化して、それに新たなIPヘッダを付加する（トンネル・モード）。一方、鍵初期化要求メッセージ及びBUがIPパケットのペイロードに配置されている場合には、暗号化／復号化部203は、IPヘッダ以外のデータ部を暗号化する（トランスポート・モード）。

#### 【0179】

又は、IPヘッダとデータ部をともに暗号化して、それに新たなIPヘッダを付加する。暗号化／復号化部203は、暗号化したBU（IPパケット）をパケット送受信部201へ渡す（S505）。

#### 【0180】

パケット送受信部201は、暗号化／復号化部203からのBU（IPパケット）を鍵送信装置（HA）100に対して送信する（S506）。

#### 【0181】

図23、図28に示すように、鍵送信装置（HA）100は、鍵受信装置（MN）200からのBU（鍵初期化要求メッセージを含むIPパケット）を受信する（S507）と、その受信パケットからSPI値を抽出する（S508）。又は、暗号化／復号化部がこのSPI値を抽出するようにしてもよい。パケット送受信部101は、その受信したパケットが暗号化されていれば暗号化／復号化部103へ渡す（S509）。

#### 【0182】

暗号化／復号化部103は、受信したパケットのSPI値及び鍵生成／管理部102を参照し、そのSPI値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（S510）、登録要求（BU）の処理後、その復号化したパケットとSPI値とをプロトコル制御部104へ渡す（S511）。

#### 【0183】

プロトコル制御部104は、鍵生成／管理部102を参照して（S512）、鍵－SPI値テーブルと抽出したSPI値とを照合することで、暗号化／復号化部103からのパケットがどの鍵で暗号化されているかを判定（S513）する

。そして、プロトコル制御部 104 は、それが初期化鍵を用いて暗号化されたことを意味していると判定したのであれば、それを鍵生成／管理部 102 に通知する (S514)。

#### 【0184】

鍵生成／管理部 102 は、新たな鍵を生成する (S515) (又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。)。鍵生成／管理部 102 は、鍵の設定を初期化するとともに、鍵-SPI 対応テーブルを初期化する (S516、S517)。

#### 【0185】

具体的には、暗号化鍵(送信用)として初期化鍵を、復号化鍵(受信用)として新たな鍵及び初期化鍵を、それぞれ設定する(図1参照)。そして、鍵生成／管理部 102 は、その鍵の設定後、その生成した新たな鍵をプロトコル制御部 104 に渡す (S518)。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

#### 【0186】

プロトコル制御部 104 は鍵配布メッセージを含む登録応答 (BA) を作成する (S519)。本実施形態では Mobile IPv6 を用いているので、例えば、プロトコル制御部 104 は、拡張ヘッダ部分 (又はペイロード部分) に鍵配布メッセージ (新たな鍵を含む) 及び BA を設定 (又は配置) した BA (IP パケット) を作成する。

#### 【0187】

この BA (IP パケット) は後述のように暗号化／復号化部 103 により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように (即ち受信側で復号できるように)、プロトコル制御部 104 は、その BA (IP パケット) に AH (authentication header) 又は ESP (encapsulating security payload) を適用する。なお、AH のみを適用した場合は、BA に含んで配布する鍵を別途暗号化 (AH で用いる鍵を流用することも可能) する必要がある。AH 又は ESP には SPI (security parameters index) のフィールドが含まれるので

、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

#### 【0188】

ここでは、後述のようにBA（IPパケット）は送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部104は、作成したBA（IPパケット）を暗号化／復号化部103へ渡す（S520）。

#### 【0189】

暗号化／復号化部103は、鍵生成／管理部102を参照して（S521）（送信用の鍵（初期化鍵）を用いて）そのBA（IPパケット）を暗号化する（S522）。暗号化／復号化部による暗号化は次のようにして行う。例えば、鍵配布メッセージ及びBAがIPv6のIPパケットの拡張ヘッダに配置されている場合には、暗号化／復号化部は、IPヘッダとデータ部をともに暗号化して、それに新たなIPヘッダを付加する（トンネル・モード）。

#### 【0190】

一方、鍵配布メッセージ及びBAがIPパケットのペイロードに配置されている場合には、暗号化／復号化部は、IPヘッダ以外のデータ部を暗号化する（トランスポート・モード）。又は、IPヘッダとデータ部をともに暗号化して、それに新たなIPヘッダを付加する。暗号化／復号化部は、暗号化したBA（IPパケット）をパケット送受信部101へ渡す（S523）。

#### 【0191】

パケット送受信部101は、暗号化／復号化部103からのBA（IPパケット）を鍵受信装置（MN）200に対して送信する（S524）。

#### 【0192】

図7、図18に示すように、鍵受信装置（MN）200は、鍵送信装置（HA）100からのBA（IPパケット）を受信する（S122）。パケット送受信部201は、受信したパケットが暗号化されていれば暗号化／復号化部203へ渡す（S123）。暗号化／復号化部203は、受信したパケットのSPI値及び鍵管理部202を参照し（S124）、そのSPI値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（S125）、プロトコル制御部20

4へ渡す(S126)。

【0193】

プロトコル制御部204は暗号化／復号化部203からのパケットの内容を判定し(S127)、鍵配布メッセージであれば鍵(HAで生成された新たな鍵)を抽出し、その抽出した鍵を鍵管理部202に渡す(S128)。

【0194】

鍵管理部202は、復号化鍵(受信用)として新たに(初期化鍵に加えて)その抽出した新たな鍵を設定する(S129)。また、鍵管理部は、暗号化鍵(送信用)として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する(初期化鍵そのものは削除されない)。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

【0195】

(8) 鍵受信装置(MN)200からのBUが鍵初期化鍵で暗号化されている場合の動作例(その2)

【0196】

図22は、鍵受信装置(MN)起動時に動的鍵(共通鍵)を配布する手順を説明するためのシーケンス図である。図5及び図7は、鍵受信装置(MN)に着目したシーケンス図である。図23は、鍵送信装置(HA)に着目したシーケンス図である。図28は、鍵送信装置(HA)における概略処理を説明するためのフローチャートである。

【0197】

ここでは、鍵送信装置(HA)100、鍵受信装置(MN)200それぞれは、最新の鍵(N番目の鍵)及び一世代前の鍵(N-1番目の鍵)を保持、管理している(図1参照)。そして、鍵送信装置(HA)100の暗号化鍵(送信用)として一世代前の鍵(N-1番目の鍵)が、鍵受信装置(MN)の暗号化鍵(送信用)として最新の鍵(N番目の鍵)が、それぞれ使用可能であるように設定されている。また、鍵送信装置(HA)100、鍵受信装置(MN)200双方の復号化鍵(受信用)として、最新の鍵(N番目の鍵)、一世代前の鍵(N-1番目の

鍵) の二つが使用可能であるように設定されている(図1参照)。

#### 【0198】

鍵受信装置(MN) 200の要求による鍵の初期化には、鍵受信装置(MN) 200の再起動時等がある。図22、図5に示すように、鍵受信装置(MN) 200は、鍵受信装置(MN) 200内部で鍵の初期化を決定した場合(S500)、BUを作成する。ここでは、上記実施形態と異なり、BUに鍵初期化要求メッセージを含まない。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部204は、拡張ヘッダ部分(又はペイロード部分)にBUを設定(又は配置)したIPパケットを作成する(S501)。

#### 【0199】

このBU(IPパケット)は後述のように暗号化/復号化部203により暗号化されるので、その暗号化に用いた鍵を受信側(HA)で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部204は、そのBU(IPパケット)にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能)する必要がある。

#### 【0200】

AH又はESPにはSPI(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにIPパケットは送信用の鍵(N番目の鍵)で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてN番目の鍵を指定するデータが設定される。プロトコル制御部204は、作成したBU(鍵初期化要求メッセージを含むIPパケット)を暗号化/復号化部203へ渡す(S502)。

#### 【0201】

暗号化/復号化部203は、鍵管理部202を参照して(S503)(送信用の鍵(N番目の鍵)を用いて)プロトコル制御部204からのBU(IPパケット)を暗号化する(S504)。この暗号化の方法についてはすでに述べた。暗号



化／復号化部 203 は、暗号化した BU (IP パケット) をパケット送受信部 201 へ渡す (S505)。

#### 【0202】

パケット送受信部 201 は、暗号化／復号化部 203 からの BU (IP パケット) を鍵送信装置 (HA) 100 に対して送信する (S506)。

#### 【0203】

図 23、図 28 に示すように、鍵送信装置 (HA) 100 は、鍵受信装置 (MN) 200 からの BU (鍵初期化要求メッセージを含む IP パケット) を受信し (S507) と、その受信パケットから SPI 値を抽出する (S508)。又は、暗号化／復号化部がこの SPI 値を抽出するようにしてもよい。そして、鍵の生成と設定の初期化を行う。

#### 【0204】

具体的には、パケット送受信部 101 は、その受信したパケットが暗号化されていれば暗号化／復号化部 103 に渡す (S509)。暗号化／復号化部 103 は、受信したパケットの SPI 値及び鍵生成／管理部 102 を参照し、その SPI 値によって指定される鍵 (ここでは N 番目の鍵) でパケットを復号し (S510)、登録要求 (BU) の処理後、その復号化したパケットと SPI 値とをプロトコル制御部 104 に渡す (S511)。

#### 【0205】

プロトコル制御部 104 は、鍵生成／管理部 102 を参照して (S512)、鍵－SPI 値テーブルと抽出した SPI 値とを照合することで、暗号化／復号化部 103 からのパケットがどの鍵で暗号化されているかを判定する (S513)。そして、プロトコル制御部 104 は、それが初期化鍵を用いて暗号化されたことを意味していると判定したのであれば、それを鍵生成／管理部 102 に通知する (S514)。

#### 【0206】

鍵生成／管理部 102 は、新たな鍵 (N+1 番目の鍵) を生成する (S515) (又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が

保持する鍵データベース等から鍵を読み出す。) 。鍵生成/管理部102は、鍵の設定を初期化するとともに、鍵-SPI対応テーブルを初期化する(S516、S517)。具体的には、鍵生成/管理部102は、復号化鍵(受信用)として新たにN+1番目の鍵と初期化鍵を設定し、N-1番目の鍵を削除する。また、鍵生成/管理部102は、暗号化鍵(送信用)として新たに初期化鍵を設定し、N-1番目の鍵を削除する。なお、初期化鍵をN-1番目の鍵として扱い、次の鍵更新時には初期化鍵を削除する。そして、鍵生成/管理部102は、鍵の設定を更新後、その作成した新たな鍵(N+1番目の鍵)をプロトコル制御部104に渡す(S518)。

#### 【0207】

プロトコル制御部104は鍵配布メッセージを含む登録応答(BA)を作成する(S519)。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部104は、拡張ヘッダ部分(又はペイロード部分)に鍵配布メッセージ(新たな鍵を含む)及びBAを設定(又は配置)したBA(IPパケット)を作成する。

#### 【0208】

このBA(IPパケット)は後述のように暗号化/復号化部103により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部104は、そのBA(IPパケット)にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能)する必要がある。AH又はESPにはSPI(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

#### 【0209】

ここでは、後述のようにIPパケットは送信用の鍵(初期化鍵)で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部104は、作成したBA(IPパケット)を暗号化/復号化部103へ渡す(S520)。

**【0210】**

暗号化／復号化部103は、鍵生成／管理部102を参照して(S521) (送信用の鍵(初期化鍵)を用いて)そのBA(IPパケット)を暗号化する(S522)。この暗号化の方法についてはすでに述べた。暗号化／復号化部103は、暗号化したIPパケットをパケット送受信部101へ渡す(S523)。

**【0211】**

パケット送受信部101は、暗号化／復号化部103からのIPパケットを鍵受信装置(MN)200に対して送信する(S524)。

**【0212】**

図7、図18に示すように、鍵受信装置(MN)200は、鍵送信装置(HA)100からのBA(鍵配布メッセージが付加されたIPパケット)を受信する(S122)。パケット送受信部201は、受信したパケットが暗号化されていれば暗号化／復号化部203へ渡す(S123)。暗号化／復号化部203は、受信したパケットのSPI値及び鍵管理部202を参照し(S124)、そのSPI値によって指定される鍵(ここでは初期化鍵)でパケットを復号化し(S125)、プロトコル制御部204へ渡す(S126)。

**【0213】**

プロトコル制御部204は暗号化／復号化部203からのパケットの内容を判定し(S127)、鍵配布メッセージであれば鍵(HAで生成された新たなN+1番目の鍵)を抽出し、その抽出した鍵を鍵管理部202に渡す(S128)。

**【0214】**

鍵管理部202は、復号化鍵(受信用)として新たに(初期化鍵に加えて)その抽出した新たな鍵を設定する(S129)。また、鍵管理部202は、暗号化鍵(送信用)として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する(初期化鍵そのものは削除されない)。

**【0215】**

(9) 鍵送信側装置(HA)が鍵の更新を判断する場合のHAの動作例

**【0216】**

図14は、鍵送信側装置(HA)が鍵の更新を判断して、動的鍵(共通鍵)を配

布する手順を説明するためのシーケンス図である。図7は、鍵受信装置(MN)に着目したシーケンス図である。図15は、鍵送信装置(HA)に着目したシーケンス図である。図18は、鍵受信装置(MN)における概略処理を説明するためのフローチャートである。図19は、鍵送信装置(HA)における概略処理を説明するためのフローチャートである。図28は、鍵送信装置(HA)における概略処理を説明するためのフローチャートである。

#### 【0217】

ここでは、鍵送信装置(HA)100が鍵の更新(タイミング)を判断するため、鍵送信装置(HA)100の鍵生成/管理部102に鍵更新タイマが内蔵されているものとし、鍵配布メッセージはMobile IPv6のBAメッセージと共に送信されるものとする。この鍵更新タイマにより、一定周期で鍵の更新を行うことが可能となる。また、鍵送信装置(HA)100はN-1番目の鍵とN番目の鍵を保持しているとし、鍵送信装置(HA)100でN+1番目の鍵が生成され、その鍵が鍵受信装置(MN)200に配布されるものとする。

#### 【0218】

図24に示すように、鍵生成/管理部102において鍵受信装置(MN)100の鍵更新タイマが満了すると(S600)、そのことをプロトコル制御部104に通知し(S601)、プロトコル制御部104はそれを鍵受信装置(MN)200ごとに保持する。例えば、プロトコル制御部104は、該当する鍵受信装置(MN)200に対する鍵更新タイマ満了フラグをオンにセットする。

#### 【0219】

鍵送信装置(HA)100は、鍵受信装置(MN)200からのBU(これには所定メッセージは含まれていない)を受信すると、BU処理を実行するとともに(S602)、その受信パケットからSPI値を抽出する(S613)。そして、暗号化/復号化部103は、受信したパケットのSPI値及び鍵生成/管理部102を参照し、そのSPI値によって指定される鍵(ここではN番目の鍵)でパケットを復号する(S614)。

#### 【0220】

プロトコル制御部104は、鍵生成/管理部102を参照して鍵-SPI値テ

ーブルと抽出したSPI値とを照合することで、受信パケットがどの鍵で暗号化されているかを判定する(S615)。そして、プロトコル制御部104は、それがN番目の鍵を用いて暗号化されたことを意味していると判定したのであれば(S616)、そのBU送信元の鍵受信装置(MN)200の鍵更新タイマが満了したか否かを判定する(S617)。

#### 【0221】

該当する鍵更新タイマが満了していれば(S617:Yes)(例えば該当する鍵受信装置(MN)200に対する鍵更新タイマ満了フラグがオンにセットされていれば)、プロトコル制御部104は、BAを作成する際、鍵生成/管理部102に鍵の更新を要求する。

#### 【0222】

鍵生成/管理部102は、新たな鍵(N+1番目の鍵)を生成する(S603)(又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこれを取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。)。鍵生成/管理部102は、鍵の設定を更新するとともに、鍵-SPI対応テーブルを更新する(S604、S605)。

#### 【0223】

具体的には、復号化鍵(受信用)として新たにN+1番目の鍵を設定し、N-1番目の鍵を削除する。また、暗号化鍵(送信用)として新たにN番目の鍵を設定し、N-1番目の鍵を削除する。そして、鍵生成/管理部102は、その鍵の設定を更新後、その生成した新たな鍵(N+1番目の鍵)をプロトコル制御部104に渡す(S606)。

#### 【0224】

プロトコル制御部104は鍵配布メッセージを含む登録応答(BA)を作成する(S607)。本実施形態ではMobile IPv6を用いているので、例えば、プロトコル制御部104は、拡張ヘッダ部分(又はペイロード部分)に鍵配布メッセージ(新たな鍵を含む)及びBAを設定(又は配置)したBA(IPパケット)を作成する。

#### 【0225】

このBA (IPパケット) は後述のように暗号化／復号化部103により暗号化されるので、その暗号化に用いた鍵を受信側(MN) で知ることができるように(即ち受信側で復号できるように)、プロトコル制御部104は、そのBA (IPパケット) にAH(authentication header)又はESP(encapsulating security payload)を適用する。なお、AHのみを適用した場合は、BAに含んで配布する鍵を別途暗号化(AHで用いる鍵を流用することも可能) する必要がある。AH又はESPにはSPI(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

#### 【0226】

ここでは、後述のようにIPパケットは送信用の鍵(N-1番目の鍵)で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてN-1番目の鍵を指定するデータが設定される。プロトコル制御部104は、作成したBA (IPパケット) を暗号化／復号化部103へ渡す(S608)。

#### 【0227】

暗号化／復号化部103は、鍵生成／管理部102を参照して(S609) (送信用の鍵(N-1番目の鍵)を用いて) そのBA (IPパケット) を暗号化する(S610)。この暗号化の方法についてはすでに述べた。暗号化／復号化部103は、暗号化したIPパケットをパケット送受信部101へ渡す(S611)。

#### 【0228】

パケット送受信部101は、暗号化／復号化部103からのIPパケット(鍵配布メッセージを含むIPパケット) を鍵受信装置(MN) に対して送信する(S612)。なお、BAの送信が完了すると、該当する鍵受信装置(MN) 200に対する鍵更新タイマ満了フラグはオフにセットされる。

#### 【0229】

図7、図18に示すように、鍵受信装置(MN) 200は、鍵送信装置(HA) 100からのBA(鍵配布メッセージが付加されたIPパケット)を受信する(S122)。鍵受信装置(MN) 200はそのIPパケット中に含まれる鍵を

暗号化鍵(送信用)/復号化鍵(受信用)に設定する (S129)。

#### 【0230】

具体的には、パケット送受信部201は、受信したパケットが暗号化されていれば暗号化/復号化部203へ渡す (S123)。暗号化/復号化部203は、受信したパケットのSPI値及び鍵管理部202を参照し (S124)、そのSPI値によって指定される鍵 (ここではN-1番目の鍵) でパケットを復号化し (S125)、プロトコル制御部204へ渡す (S126)。

#### 【0231】

プロトコル制御部204は暗号化/復号化部203からのパケットの内容を判定し (S127)、鍵配布メッセージであれば鍵 (HAで生成された新たなN+1番目の鍵) を抽出し、その抽出した鍵を鍵管理部202に渡す (S128)。

#### 【0232】

鍵管理部202は、復号化鍵 (受信用) として新たにその抽出した新たな鍵を設定する (S129)。また、鍵管理部202は、暗号化鍵 (送信用) として新たにその抽出した新たな鍵を設定し、送信用として設定されていた鍵を削除する。

#### 【0233】

(10) 鍵配布メッセージが破棄された場合のMNの動作例

#### 【0234】

図25は、鍵受信装置 (MN) からの鍵再送要求メッセージにより、動的鍵 (共通鍵) を配布する手順を説明するためのシーケンス図である。図26及び図7は、鍵受信装置 (MN) に着目したシーケンス図である。図27は、鍵送信装置 (HA) に着目したシーケンス図である。

#### 【0235】

ここでは、鍵送信装置 (HA) 100からの鍵配布メッセージ (N+1番目の鍵を含む) を含むBA (IPパケット) が、鍵受信装置 (MN) 200に到達せずに、途中で破棄されたものとする (図22、図26参照)。この場合、鍵送信側装置 (HA) 100のみ動的に更新される鍵が更新された状態となる (図16参照)。図28は、鍵送信装置 (HA) における概略処理を説明するためのフロー

チャートである。

#### 【0236】

図25、図26に示すように、鍵受信装置(MN)200は、鍵送信装置(HA)100に対して送信したBU(IPパケット)に対するBA(IPパケット)を受信しないこと(例えばBU送信後の一定期間内にBAを受信しないこと)を感知すると(S700)、再送のためのBU(鍵再送要求メッセージを含むIPパケット)を上記鍵更新要求メッセージ等と同様にプロトコル制御部204によって作成し(S701)、これを暗号化/復号化部203へ渡す(S702)。

#### 【0237】

暗号化/復号化部203は、鍵管理部202を参照して(S703)(送信用の鍵(N番目の鍵)を用いて)プロトコル制御部204からのBU(IPパケット)を暗号化する(S704)。この暗号化の方法についてはすでに述べた。暗号化/復号化部203は、暗号化したBU(IPパケット)をパケット送受信部201へ渡す(S705)。

#### 【0238】

パケット送受信部201は、暗号化/復号化部203からのBU(IPパケット)を鍵送信装置(HA)100に対して送信する(S706)。

#### 【0239】

図27に示すように、鍵送信装置(HA)100は、鍵受信装置(MN)200からのBU(これには鍵再送要求メッセージを含まない)を受信すると(S707)、その受信パケットからSPI値を抽出する(S708)。又は、暗号化/復号化部がこのSPI値を抽出するようにしてもよい。

#### 【0240】

具体的には、パケット送受信部101は、その受信したパケットが暗号化されていれば暗号化/復号化部103に渡す(S709)。暗号化/復号化部103は、受信したパケットのSPI値及び鍵生成/管理部102を参照し(S710)、そのSPI値によって指定される鍵(ここではN番目の鍵)でパケットを復号し(S711)、登録要求(BU)の処理後、その復号化したパケットとSP



I 値とをプロトコル制御部 104 に渡す (S712)。

【0241】

プロトコル制御部 104 は、鍵生成/管理部 102 を参照して (S713)、鍵-SPI 値テーブルと抽出した SPI 値とを照合することで、暗号化/復号化部 103 からのパケットがどの鍵で暗号化されているかを判定する (S714)。そして、プロトコル制御部 104 は、それが N 番目の鍵であれば、鍵受信装置 (MN) 200 が N+1 番目の鍵 (最新の鍵) を受信していないと判断できるため (鍵再送要求メッセージ受信に相当する)、それを鍵生成/管理部 102 に通知する (S715)。

【0242】

鍵生成/管理部 102 は、新たな鍵を生成すること無く、前回配布して途中で破棄された最新の鍵 (N+1 番目の鍵) をプロトコル制御部 104 に渡す (S716)。

【0243】

プロトコル制御部 104 は鍵配布メッセージを上記と同様に作成する (S717)。プロトコル制御部 104 は、作成した BA (IP パケット) を暗号化/復号化部 103 へ渡す (S718)。

【0244】

暗号化/復号化部 103 は、鍵生成/管理部 102 を参照して (S719) (送信用の鍵 (N 番目の鍵) を用いて) その BA (IP パケット) を暗号化する (S720)。この暗号化の方法についてはすでに述べた。暗号化/復号化部 102 は、暗号化した BA (IP パケット) をパケット送受信部 101 へ渡す (S721)。

【0245】

パケット送受信部 101 は、暗号化/復号化部からの BA (IP パケット) を鍵受信装置 (MN) 200 に対して送信する (S722)。

【0246】

図 7、図 18 に示すように、鍵受信装置 (MN) 200 は、鍵送信装置 (HA) 100 からの BA (鍵配布メッセージが付加された IP パケット) を受信する

(S122)。鍵受信装置(MN)200は、上記と同様にそのIPパケット中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する(S123～S129)。

以上述べたように、本動作例では、鍵送信側装置(HA)100は一世代前の動的鍵を暗号化鍵(送信用)として使用することにより、動的鍵配布メッセージ(鍵配布メッセージともいう)が破棄されても通信が可能となる。

#### 【0247】

(11) 鍵送信側装置(HA)の障害時等の鍵初期化手順

#### 【0248】

鍵送信装置(HA)100の障害時等の鍵の初期化手順は以下である。

#### 【0249】

ここでは、鍵送信装置(HA)100の障害等により鍵送信装置(HA)の動的に更新される鍵(N番目の鍵及びN-1番目の鍵)はすべて失われ、初期化用鍵のみが設定されているものとする。一方、鍵受信装置(MN)は動的に更新される鍵(N番目の鍵及びN-1番目の鍵)を保持しているものとする。

#### 【0250】

鍵受信装置(MN)100は、鍵送信装置(HA)100に対して送信したBU(鍵更新要求メッセージ等を含まない)に対するBA(IPパケット)を一定期間後も受信しないことを検知すると、鍵送信装置(HA)100の障害等が考えられるため、BU(鍵更新要求メッセージを含まない)を再送する。

#### 【0251】

鍵受信装置(MN)200は、その再送したBU(IPパケット)に対するBAを一定期間後も受信しないことを検知すると、動的に更新される鍵の設定を初期化し、BUを図5に示すように生成して(S501～S505)鍵送信装置(HA)100に送信する(S506)。

#### 【0252】

鍵送信装置(HA)100は、図22及び図23に示すように、鍵受信装置(MN)からのBUが初期化鍵を用いて暗号化されたことを意味していると判定すると(S507～S514)、上記と同様に、鍵の生成等の処理を行い(S51

5～S518)、BAに最新の鍵を含んだ鍵配布メッセージを付加し(S519)、鍵受信装置(MN)に送信する(S520～S524)。

#### 【0253】

図7、図18に示すように、鍵受信装置(MN)は、鍵配布メッセージが付加されたBAを受信すると(S122)、その中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する(S123～S129)。これについてはすでに述べたものと同様である。

#### 【0254】

以上述べたように、本動作例によれば、鍵受信装置(MN)200が鍵更新要求メッセージ又はそれに相当するメッセージを再送することにより、正常な状態(最新の鍵が鍵受信装置(MN)200の送受信用に設定された状態)に復帰することが可能となる。また、鍵更新要求メッセージを再送してもその返答として鍵配布メッセージが鍵受信装置に届かない場合、鍵受信装置(MN)200は鍵初期化要求メッセージを鍵送信装置(HA)100に送信することによって、初期化を行う。

#### 【0255】

以上述べたように、本動作例では、鍵受信側装置の障害等で鍵受信側装置と鍵送信側装置の動的鍵の不一致が起きた場合、動的鍵初期化メッセージ又はそれに相当するメッセージを鍵受信側装置が送信することにより、双方の動的鍵を初期化することが可能となる。

#### 【0256】

次に変形例について説明する。

#### 【0257】

上記2つの実施形態においては、鍵送信装置及び鍵受信装置間の通信は、Mobile IPv6による通信であるように説明したが、本発明はこれに限定されない。鍵送信装置及び鍵受信装置間の通信として各種の通信を適用することが可能である。例えば、鍵送信装置及び鍵受信装置間の通信は、Mobile IPv4による通信であってもよい。この場合、登録要求としてIPv6のBUに代えてRegistration Requestを、登録応答としてIPv6のBAに代えてRegist

ration Replyを、それぞれ用いる。これらは、例えば、IPパケットのペイロード部分に設定（又は配置）される。

#### 【0258】

また、上記2つの実施形態においては、鍵受信装置（MN）200から鍵送信装置（HA）100へはBU及び所定メッセージ（又はBUのみ）が送信され、これに応じて、鍵送信装置（HA）100が鍵配布メッセージを鍵受信装置（MN）200に対して配布するように説明したが、本発明はこれに限定されない。例えば、鍵受信装置（MN）200から鍵送信装置（HA）100へは所定メッセージ（例えば鍵初期化要求メッセージ）のみを送信し、これに応じて、鍵送信装置（HA）100が鍵配布メッセージを鍵受信装置（MN）200に対して配布するようにしてもよい。

#### 【0259】

また、上記2つの実施形態においては、鍵送信装置（HA）100と鍵受信装置（MN）200とがそれぞれ、共通の鍵であって世代の異なる鍵を送信用の鍵として設定するように説明したが、本発明はこれに限定されない。例えば、鍵送信装置（HA）100に送信用鍵としてN-1世代のA鍵を、鍵受信装置（MN）200に送信用鍵としてN世代のB鍵を、それぞれ設定する。そして、鍵送信装置（HA）100に受信用鍵としてN世代及びN-1世代のB鍵を、そして、鍵受信装置（MN）200に受信用としてN世代及びN-1世代のA鍵を、それぞれ設定するようにしてもよい。

#### 【0260】

また、上記2つの実施形態においては、鍵送信装置がMobile IPにおけるHAであり、鍵受信装置がMobile IPにおけるMNであるように説明したが、本発明はこれに限定されない。例えば、鍵送信装置がインターネット上のサーバ装置であり、鍵受信装置がそのサーバと通信を行うクライアント装置であってもよい。

#### 【0261】

なお、上記2つの実施形態においては、BU及びBAがIPv6の拡張ヘッダ部分（又はペイロード部分）に設定（又は配置）されるように説明したが、本発

明はこれに限定されない。IPv6の仕様については、現状ドラフトの段階である。例えば、ドラフト15版(draft-ietf-mobileip-ipv6-15.txt)においては、BU/BA共 終点オプション(destination option)に含まれる。また、ドラフト18版(draft-ietf-mobileip-ipv6-18.txt)においては、BU/BA共 モビリティヘッダ(mobility header)に含まれる。従って、BU、BAの設定(配置)は、仕様の変化に応じて適宜に改良することが可能である。

### 【0262】

[その他] 本発明は、以下のように特定することができる。

(付記1) 鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第1保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第1設定手段と、を備え、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第2保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第2設定手段と、を備える、共通鍵暗号化通信システム。(1)

(付記2) 前記鍵送信装置は、暗号化鍵を取得する取得手段をさらに備え、前記第1保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第1設定手段は、前記第1保持手段による更新後の保持鍵に基づいて、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、付記1に記載の共通鍵暗号化通信システム。(2)

(付記3) 前記鍵送信装置は、暗号化鍵を生成する生成手段を備え、前記取得手段は、前記生成手段によって生成された暗号化鍵を取得する、付記2に記載の共通鍵暗号化通信システム。(3)

(付記4) 前記鍵送信装置は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する第1送信手段をさらに備える、付記2に記載の共通鍵暗

号化通信システム。(4)

(付記5) 前記鍵受信装置は、前記鍵送信装置から送信される暗号化鍵を受信する第2受信手段をさらに備え、前記第2受信手段が暗号化鍵を受信した場合、前記第2保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記第2受信手段によって受信した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第2設定手段は、前記第2保持手段による更新号の保持鍵に基づいて、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、付記4に記載の共通鍵暗号化通信システム。(5)

(付記6) 前記鍵受信装置は、所定メッセージを鍵送信装置に対して送信する第2送信手段を備え、前記鍵送信装置は、前記鍵受信装置から送信される所定メッセージを受信する第1受信手段を備える、付記1に記載の共通鍵暗号化システム。(6)

(付記7) 前記第1及び第2保持手段は、それぞれ初期化鍵を保持する、付記4に記載の共通鍵暗号化通信システム。(7)

(付記8) 前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵初期化要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵初期化要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第1保持手段は、共通の初期化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する、付記7に記載の共通鍵暗号化通信システム。

(付記9) 前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵更新要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵更新要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第1保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する、付記4に記載の共通鍵暗号化通信システム。

(付記10) 前記鍵受信装置は、鍵更新時期を決定するための手段を備え、前記第2送信手段は、鍵更新時期に達した場合に、鍵更新要求メッセージを鍵送信

装置に対して送信する、付記 9 に記載の共通鍵暗号化通信システム。

(付記 11) 前記鍵送信装置は、鍵更新時期を決定するための手段を備え、第 1 送信手段は、鍵更新時期に達した場合に、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する、付記 4 に記載の共通鍵暗号化通信システム。

(付記 12) 前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵再送要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵再送要求メッセージを受信した場合、第 1 送信手段は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する、付記 4 に記載の共通鍵暗号化通信システム。

(付記 13) 前記第 1 送信手段は、前記第 1 及び第 2 保持手段がいずれの鍵も保持していない状態で、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する、請求項 4 に記載の共通鍵暗号化通信システム。

(付記 14) 鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵送信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵送信装置。(8)

(付記 15) 鍵送信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵受信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵受信装置。(9)

(付記 16) 鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う方法であって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定し、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵

及び一世代前の暗号化鍵を、それぞれ設定する、共通鍵暗号化通信方法。(10)

### 【0263】

本発明は、その精神または主要な特徴から逸脱することなく、他の様々な形で実施することができる。このため、上記の実施形態はあらゆる点で単なる例示にすぎず、これらの記載によって本発明が限定的に解釈されるものではない。

### 【0264】

#### 【発明の効果】

以上説明したように、本発明によれば、共通鍵暗号化通信を行う二つの装置の一方が他方に暗号化鍵を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も暗号化通信を継続することが可能となる。また、一対多の暗号化通信（例えばMobile IPにおけるMNとHA間や、インターネット上のサーバとそれに接続するクライアント間等の通信）を行う場合に、HAやインターネット上のサーバの負荷の低減が可能となる。またセキュリティを高めるための動的な鍵更新を行った場合も、それに伴って通信断が発生しない。

#### 【図面の簡単な説明】

#### 【図1】

本発明の実施の形態である共通鍵暗号化通信システムの概略構成を説明するための図である。

#### 【図2】

鍵送信装置（HA）の構成例を説明するための図である。

#### 【図3】

鍵受信装置（MN）の構成例を説明するための図である。

#### 【図4】

鍵受信装置（MN）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

#### 【図5】

鍵受信装置（MN）に着目したシーケンス図である。

#### 【図6】



鍵送信装置（H A）に着目したシーケンス図である。

【図 7】

鍵受信装置（M N）に着目したシーケンス図である。

【図 8】

鍵受信装置（M N）からの鍵更新要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図 9】

鍵受信装置（M N）に着目したシーケンス図である。

【図 1 0】

鍵送信装置（H A）に着目したシーケンス図である。

【図 1 1】

鍵受信装置（M N）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図 1 2】

鍵受信装置（M N）に着目したシーケンス図である。

【図 1 3】

鍵送信装置（H A）に着目したシーケンス図である。

【図 1 4】

鍵送信側装置（H A）が鍵の更新を判断して、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図 1 5】

鍵送信装置（H A）に着目したシーケンス図である。

【図 1 6】

鍵送信装置（H A）のみ鍵が更新された状態を説明するための図である。

【図 1 7】

鍵送信装置（H A）における概略処理を説明するためのフローチャートである。

【図 1 8】

鍵受信装置（M N）における概略処理を説明するためのフローチャートである。

。

【図 1 9】

鍵送信装置（H A）における概略処理を説明するためのフローチャートである

。

【図 2 0】

鍵受信装置（M N）における概略処理を説明するためのフローチャートである

。

【図 2 1】

鍵－S P I 対応テーブルの例を説明するための図である。

【図 2 2】

鍵受信装置（M N）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図 2 3】

鍵送信装置（H A）に着目したシーケンス図である。

【図 2 4】

鍵送信装置（H A）に着目したシーケンス図である。

【図 2 5】

鍵受信装置（M N）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図 2 6】

鍵受信装置（M N）に着目したシーケンス図である。

【図 2 7】

鍵送信装置（H A）に着目したシーケンス図である。

【図 2 8】

鍵送信装置（H A）における概略処理を説明するためのフローチャートである

。

【符号の説明】

1 0 0      鍵送信装置

1 0 1      パケット送受信部

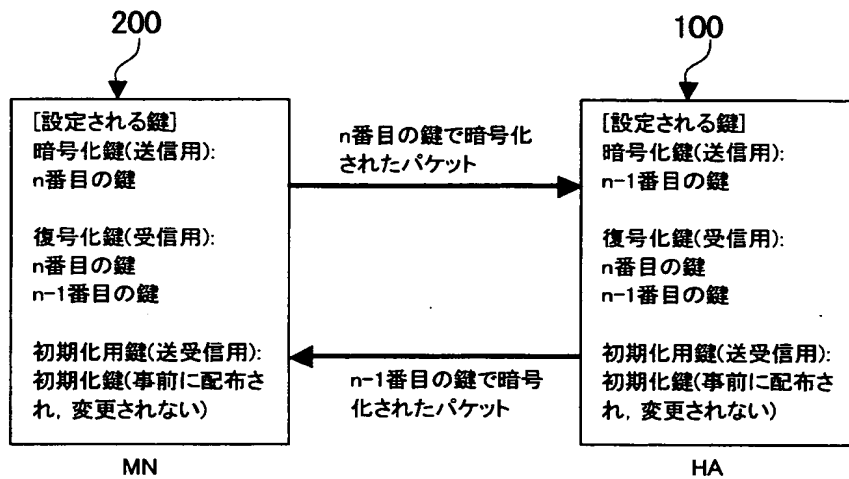
1 0 2	鍵生成／管理部
1 0 3	暗号化／復号化部
1 0 4	プロトコル制御部
2 0 0	鍵受信装置
2 0 1	パケット送受信部
2 0 2	鍵管理部
2 0 3	暗号化／復号化部
2 0 4	プロトコル制御部

【書類名】

図面

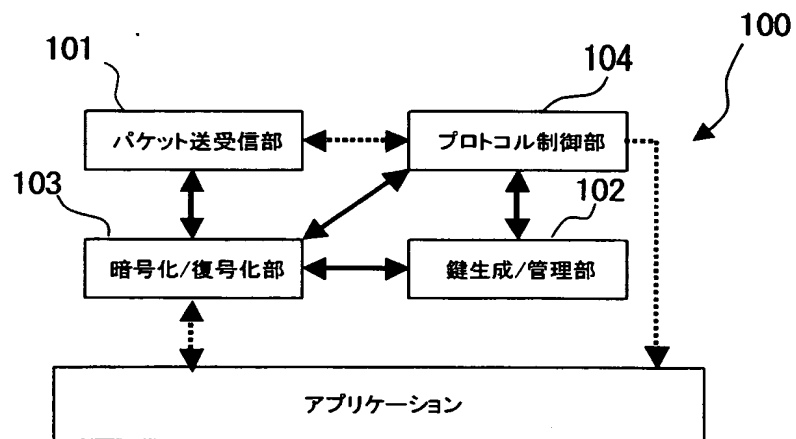
【図 1】

本発明の実施の形態である共通鍵暗号化通信システムの概略構成を説明するための図  
(動的鍵を用いた暗号化通信(定常状態))



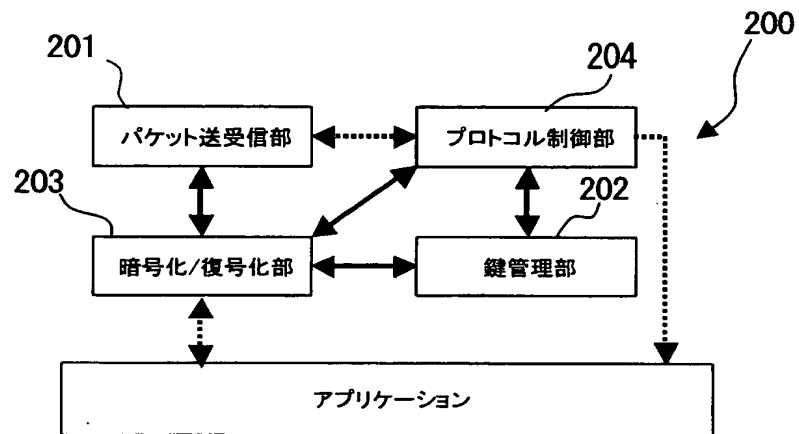
【図 2】

鍵送信装置 (HA) の構成例を説明するための図である (鍵送信側装置 (HA) の構成例)



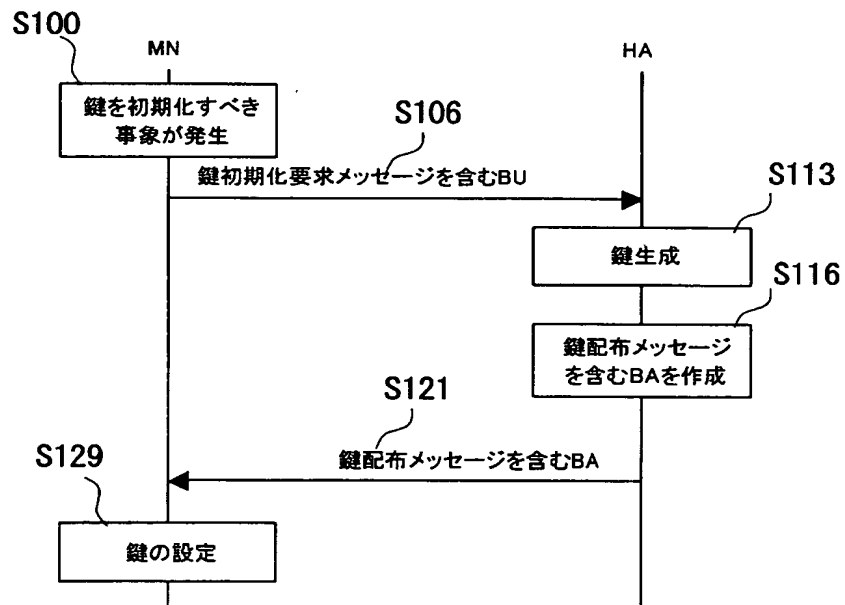
【図 3】

鍵受信装置 (MN) の構成例を説明するための図である (鍵受信側装置 (MN) の構成例)



【図 4】

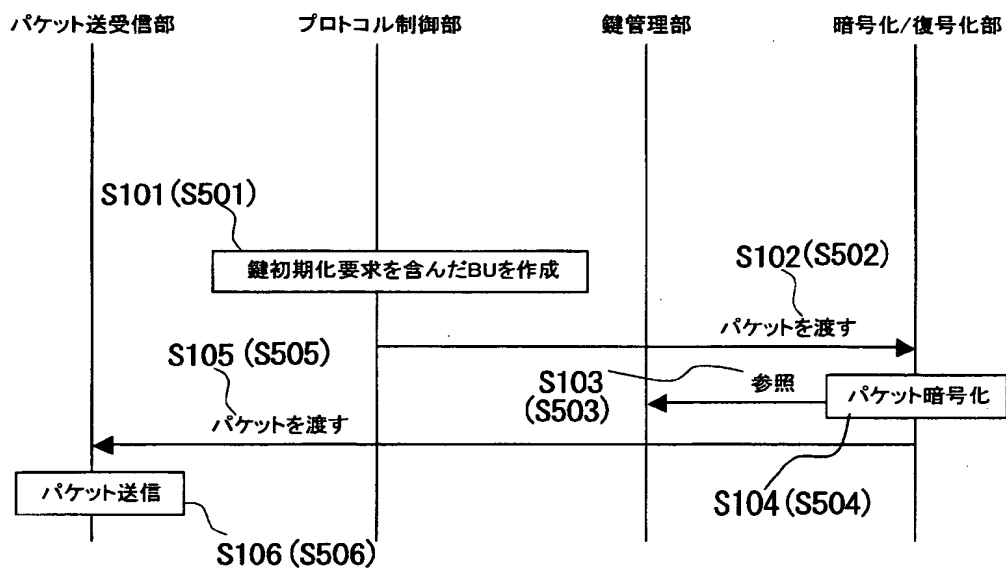
鍵受信装置 (MN) 起動時に動的鍵 (共通鍵) を配布する手順を説明するためのシーケンス図  
(鍵初期化シーケンス (鍵初期化要求メッセージを用いる場合))



【図 5】

## 鍵受信装置 (MN) に着目したシーケンス図

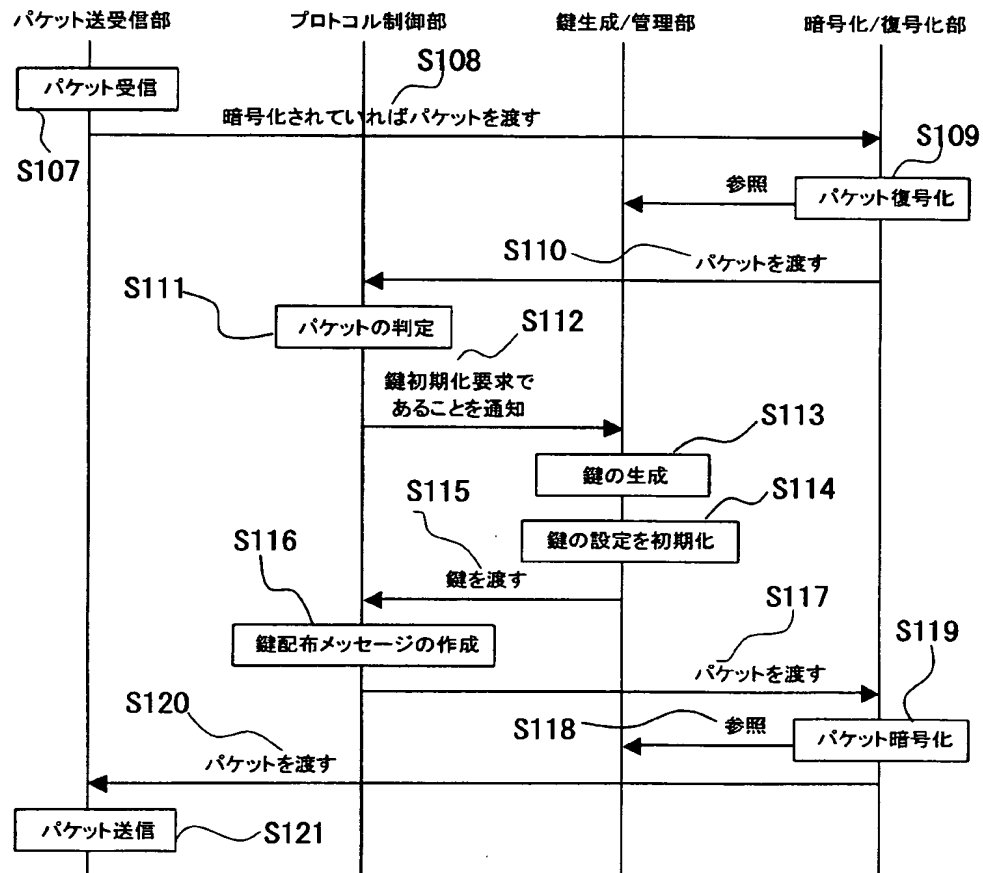
(MN が鍵の更新を判断する場合のシーケンス (鍵初期化メッセージを用いる場合))





【図 6】

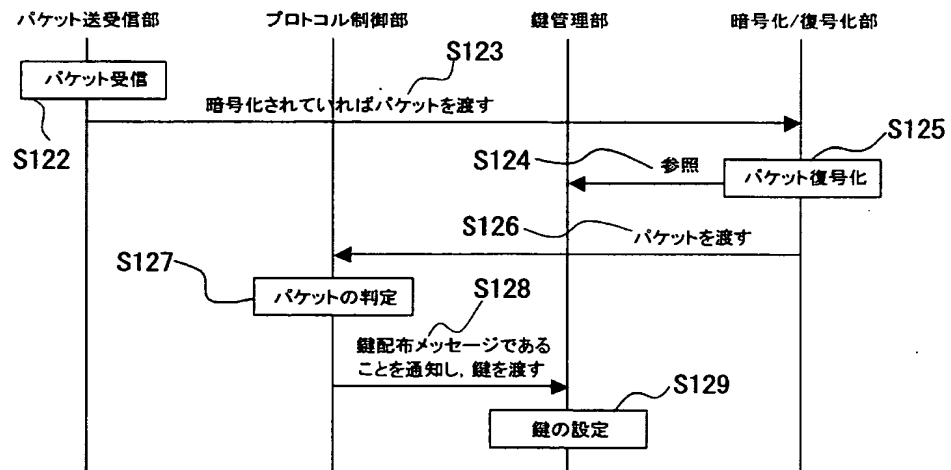
鍵送信装置（HA）に着目したシーケンス図  
（HA が鍵初期化要求メッセージを受信した場合のシーケンス）



【図 7】

鍵受信装置 (MN) に着目したシーケンス図

(鍵配布メッセージ受信時の MN のシーケンス)



【図 8】

鍵受信装置 (MN) からの鍵更新要求メッセージにより、動的鍵 (共通鍵) を配布する手順を説明するためのシーケンス図 (MN が鍵更新の契機を判断する場合の鍵配布シーケンス (鍵更新要求メッセージを用いる場合))

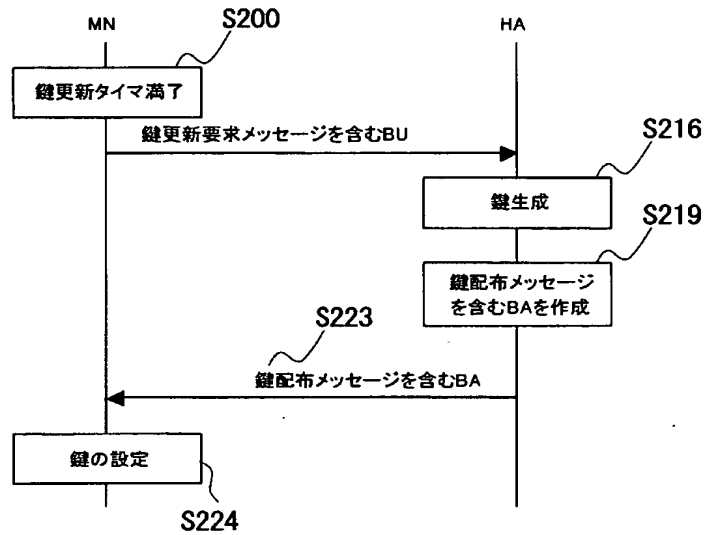
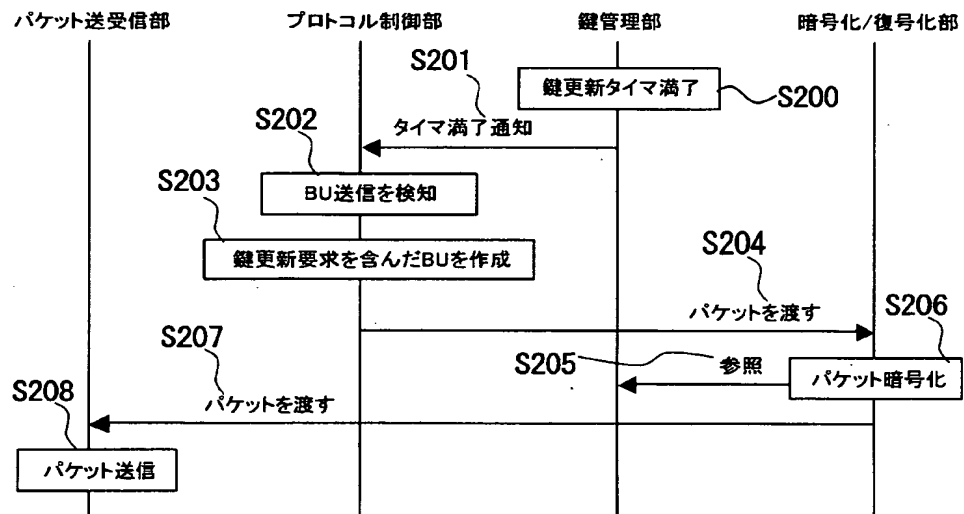


図 1:

【図 9】

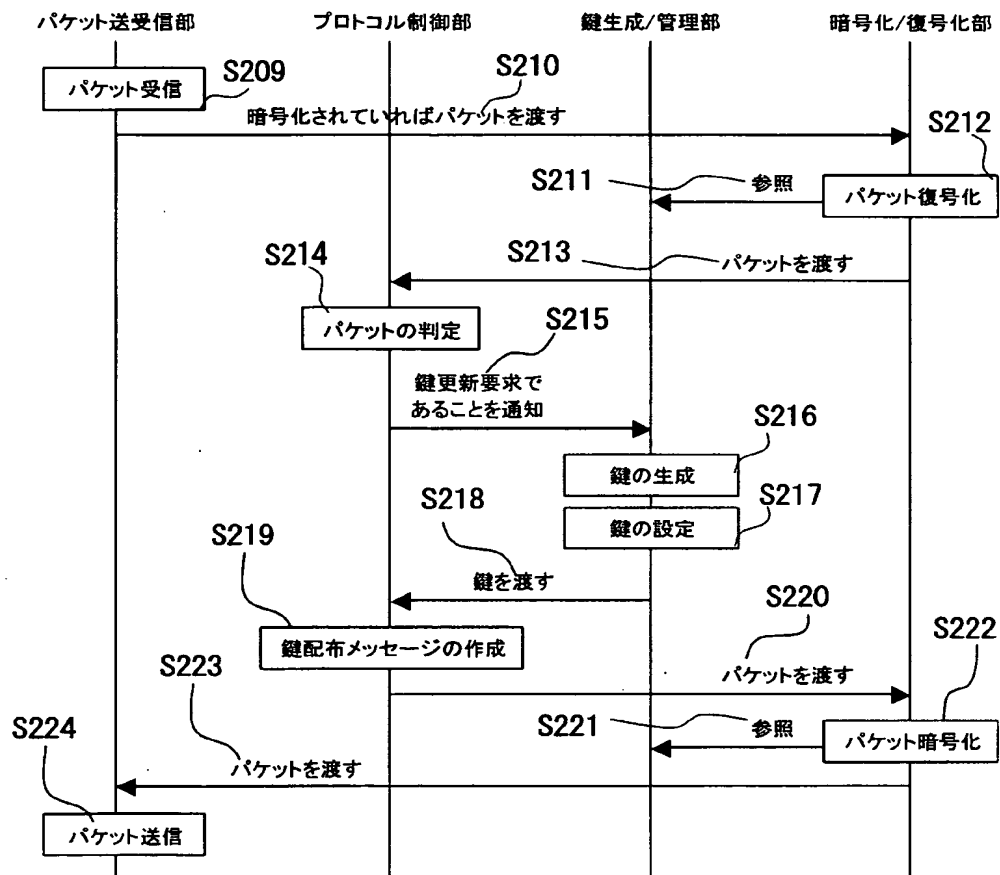
## 鍵受信装置 (MN) に着目したシーケンス図

(MN が鍵の更新を判断する場合のシーケンス (鍵更新メッセージを用いる場合))



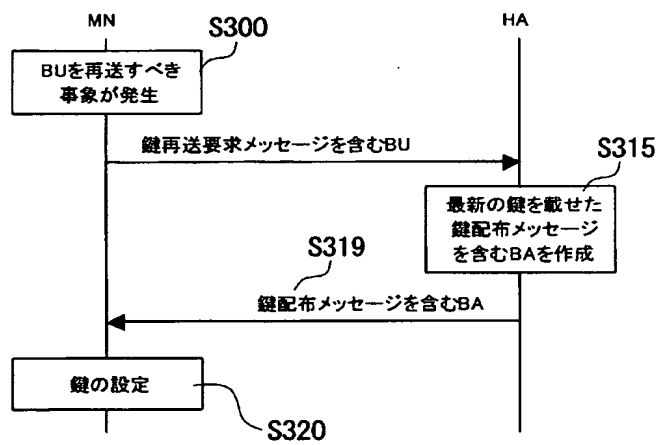
【図 10】

鍵送信装置 (HA) に着目したシーケンス図  
(HA が鍵更新要求メッセージを受信した場合のシーケンス)



【図 11】

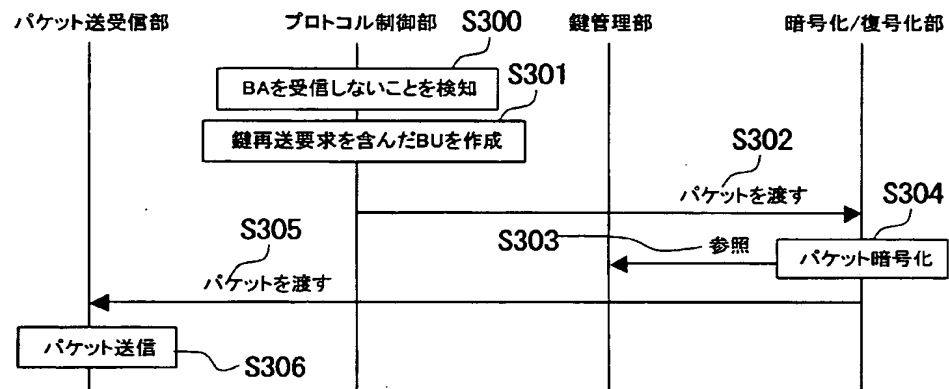
鍵受信装置 (MN) からの鍵再送要求メッセージにより、動的鍵 (共通鍵) を配布する手順を説明するためのシーケンス図 (BU 再送時の鍵配布シーケンス (再送前の BU が鍵更新/鍵再送要求メッセージだった場合))



【図 12】

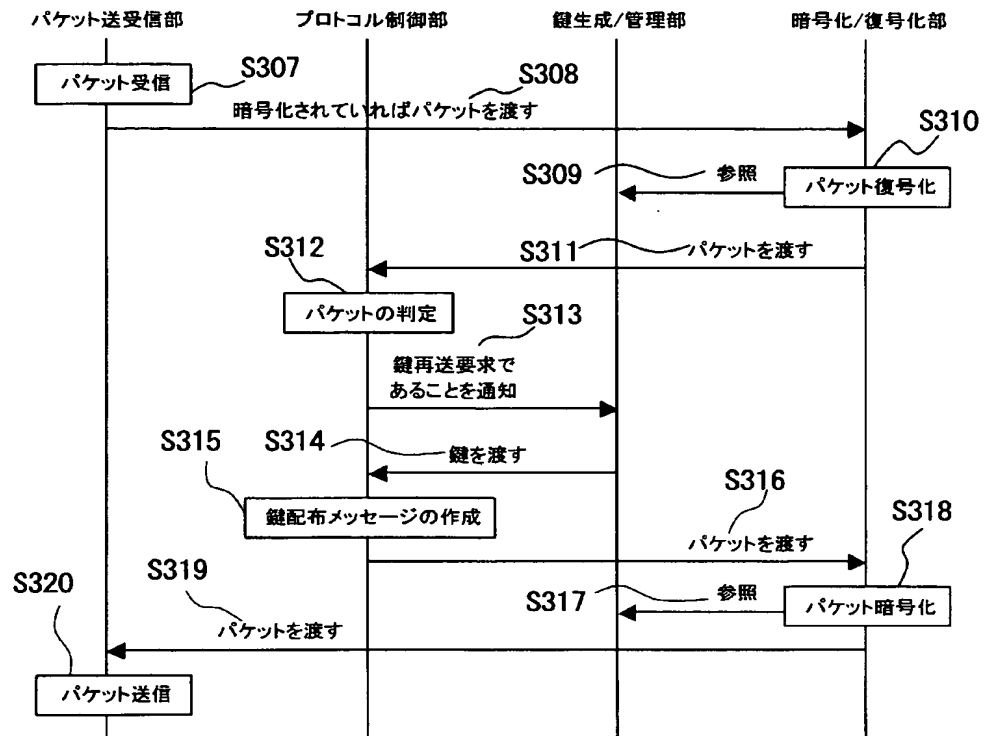
## 鍵受信装置 (MN) に着目したシーケンス図

(鍵配布メッセージが破棄された場合に MN のシーケンス (鍵再送メッセージを用いる場合))



【図 13】

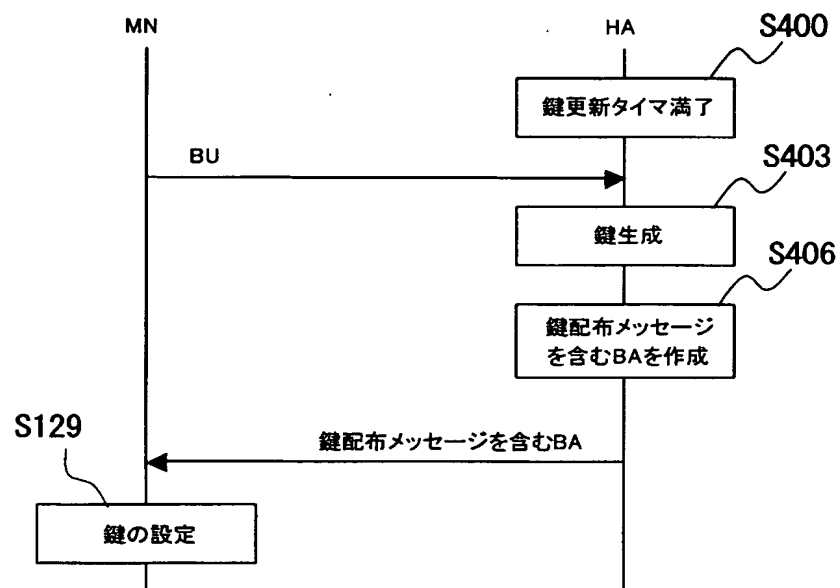
鍵送信装置（HA）に着目したシーケンス図  
（HA が鍵再送要求メッセージを受信した場合のシーケンス）





【図 14】

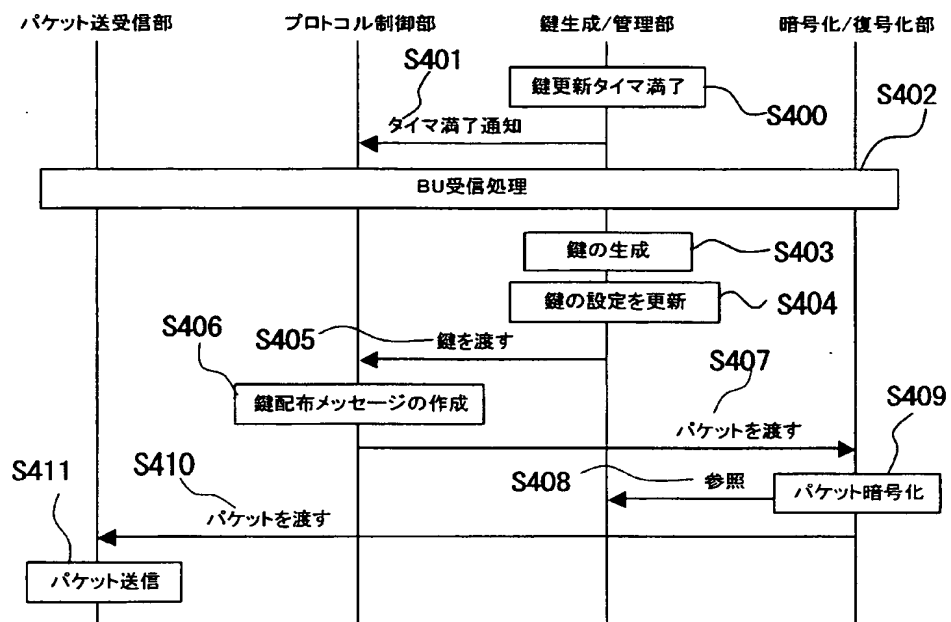
鍵送信側装置(HA)が鍵の更新を判断して、動的鍵(共通鍵)を配布する手順を説明するためのシーケンス図(HAが鍵更新の契機を判断する場合の鍵配布シーケンス)



【図 15】

## 鍵送信装置 (HA) に着目したシーケンス図

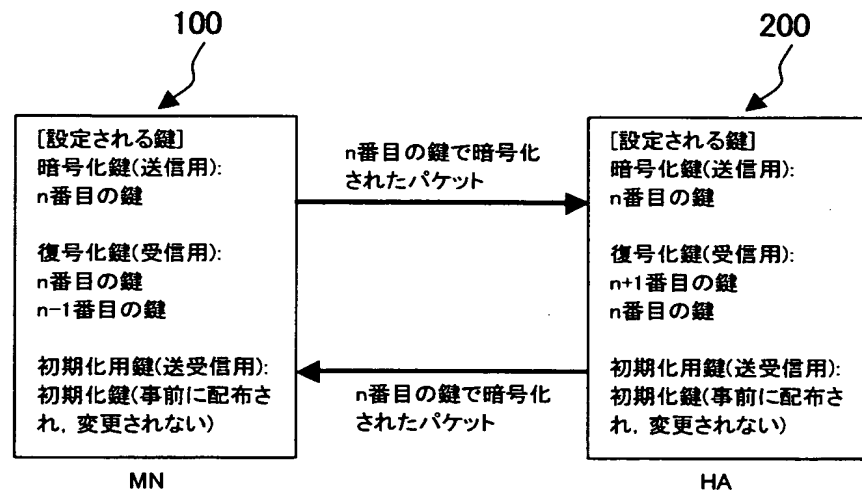
(HA が鍵の更新を判断する場合のシーケンス (鍵更新/初期化/再送メッセージを用いる場合))



【図 1 6】

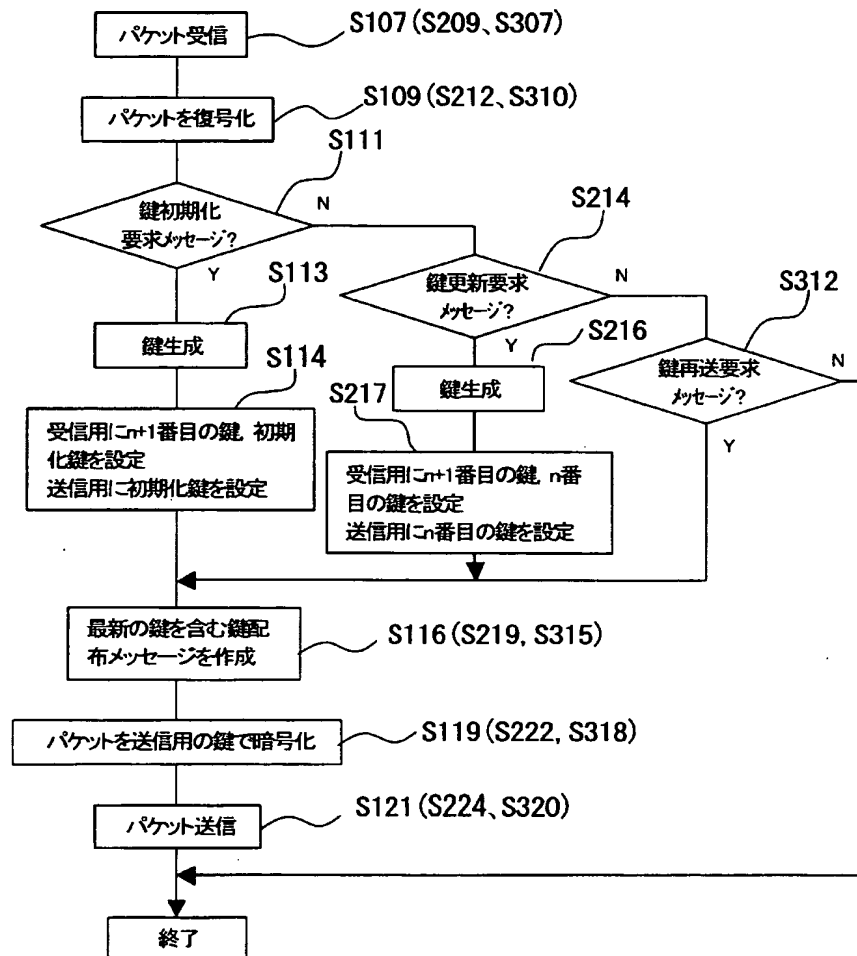
鍵送信装置（HA）のみ鍵が更新された状態を説明するための図

（ 動的鍵を用いた暗号化通信（HA のみ鍵が更新された状態））



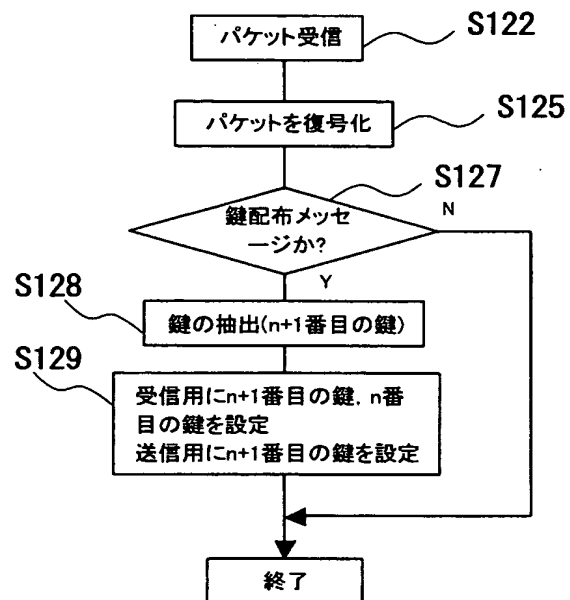
【図 17】

鍵送信装置（HA）における概略処理を説明するためのフローチャート  
（パケット受信時の鍵送信側装置（HA）での処理フロー（鍵初期化/更新/再送要求メッセージを用いる場合））



【図 18】

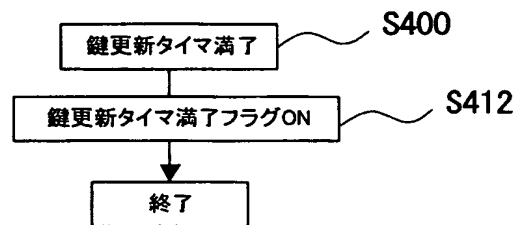
鍵受信装置 (MN) における概略処理を説明するためのフローチャート  
(パケット受信時の鍵受信側装置 (MN) での処理フロー)



【図 19】

鍵送信装置（HA）における概略処理を説明するためのフローチャート

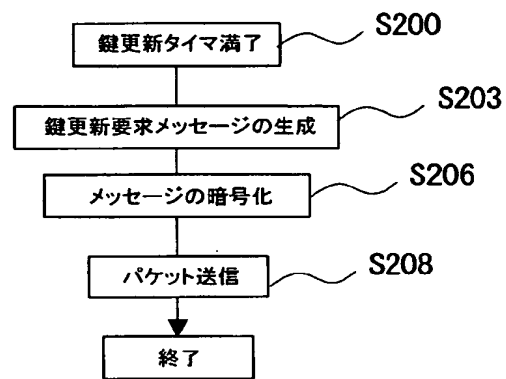
（HA が持つ鍵更新タイマ満了時の処理フロー（HA が鍵の更新を判断する場合））



【図 20】

鍵受信装置 (MN) における概略処理を説明するためのフローチャート

(MN が持つ鍵更新タイマ満了時の処理フロー (MN が鍵の更新を判断し、鍵更新要求メッセージを用いる場合))



## 【図 2 1】

鍵-SPI 対応テーブルの例を説明するための図

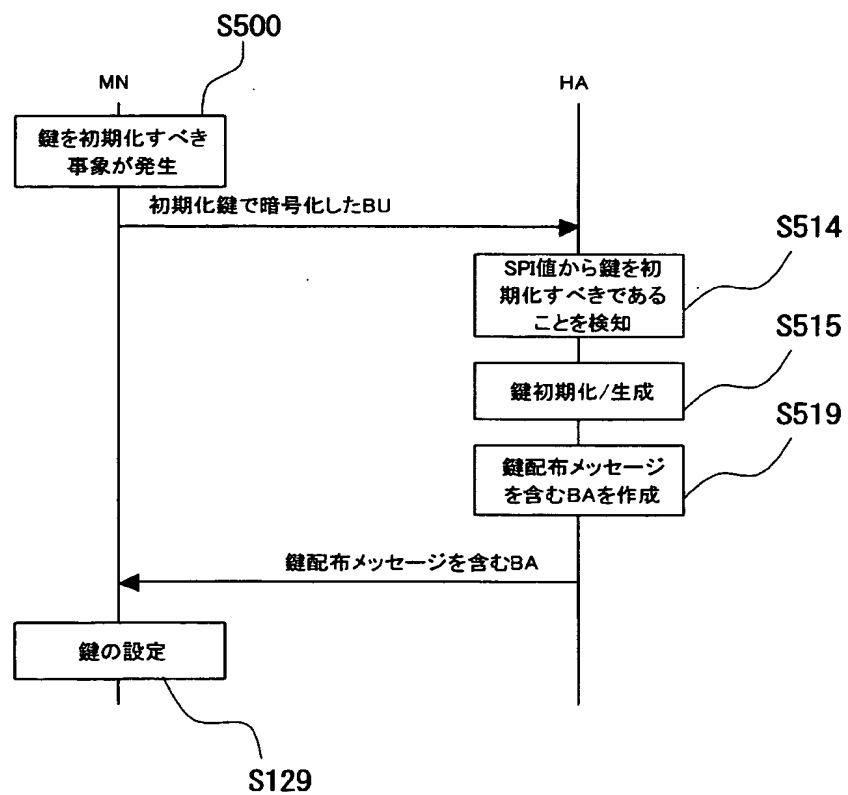
( 鍵-SPI 対応テーブル)

鍵	SPI
初期化鍵	1001
n-1 番目の鍵	2001
n 番目の鍵	2002



【図 22】

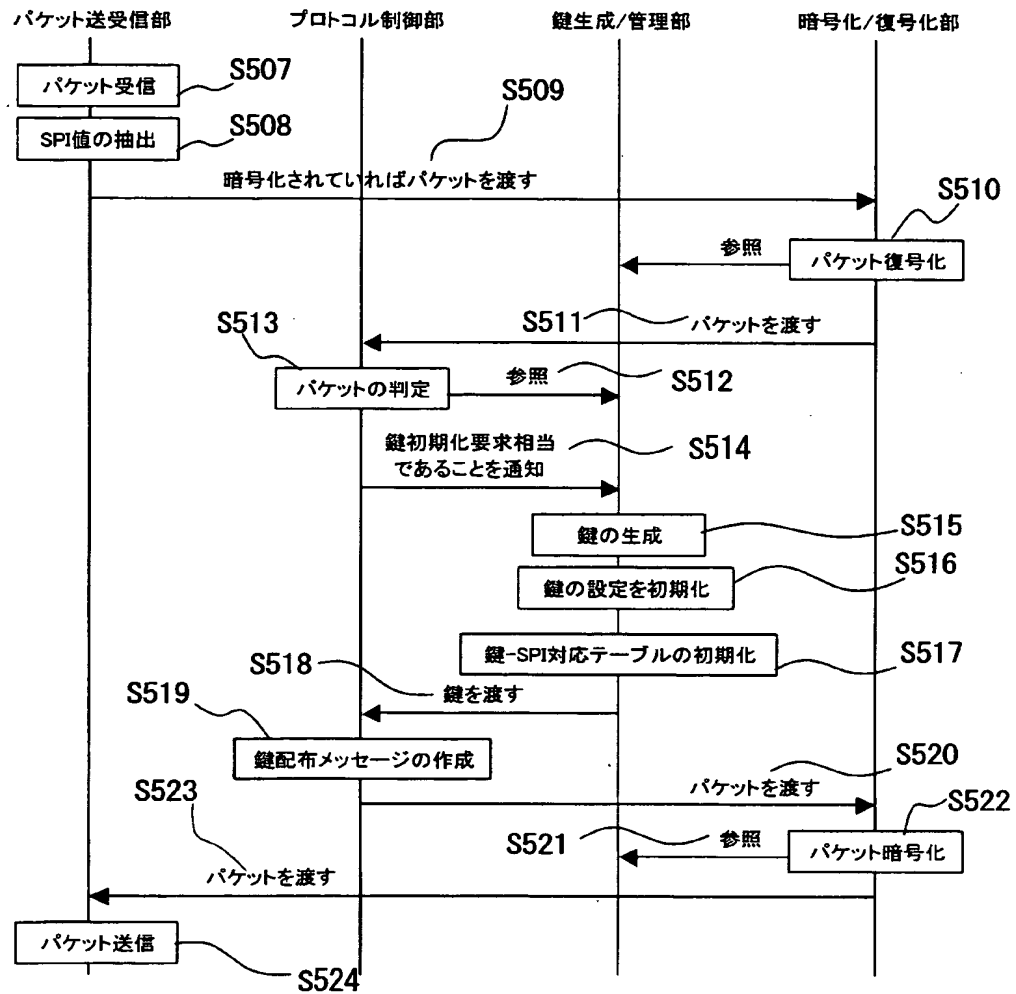
鍵受信装置（MN）起動時に動的鍵（共通鍵）を配布する手順を説明するための  
シーケンス図（鍵初期化シーケンス（SPI 値で鍵初期化を判断する場合））



【図 23】

## 鍵送信装置 (HA) に着目したシーケンス図

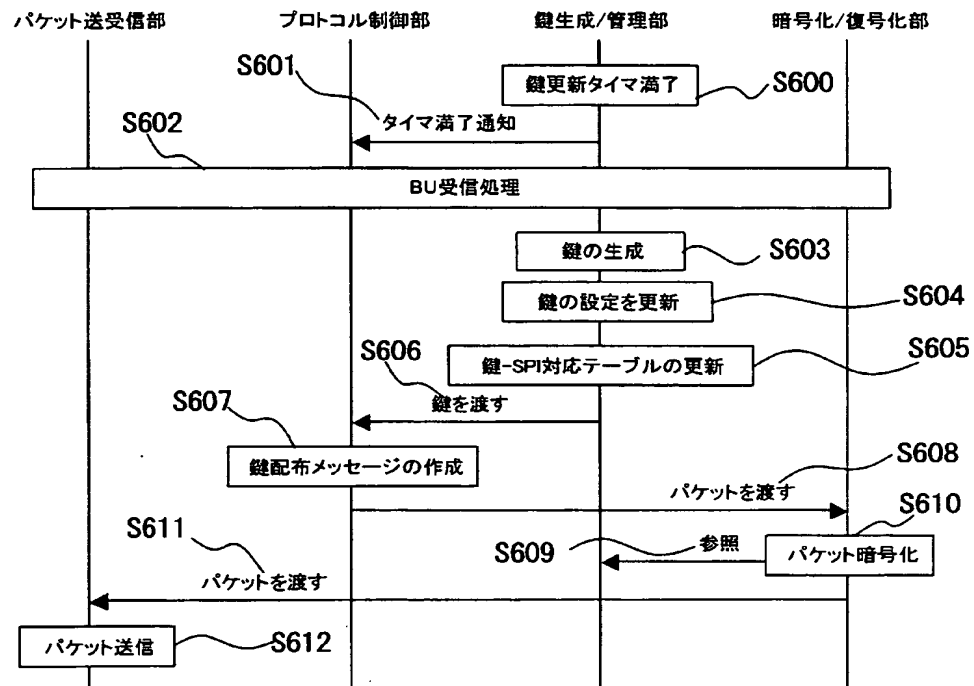
(HA が鍵初期化要求メッセージ相当の BU を受信した場合のシーケンス)



【図 24】

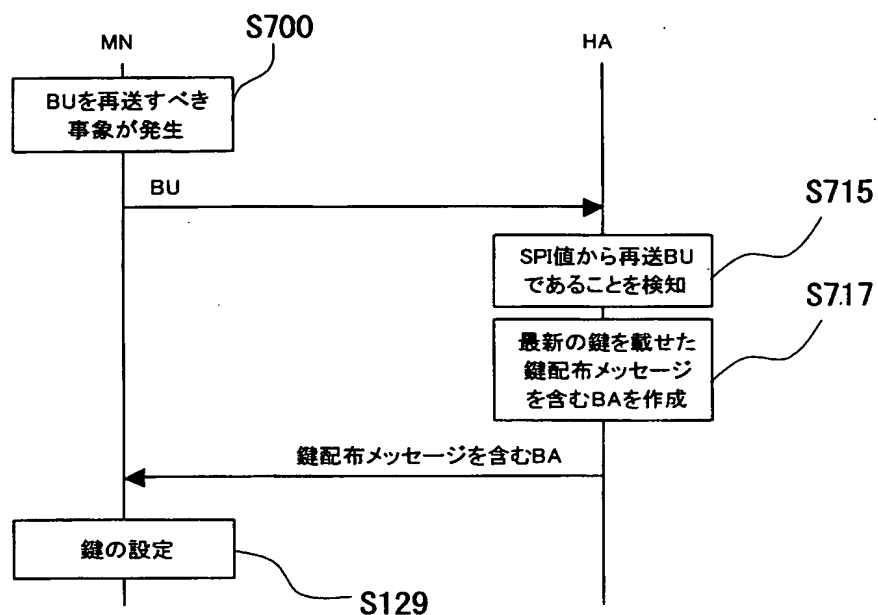
## 鍵送信装置 (HA) に着目したシーケンス図

(HA が鍵の更新を判断する場合のシーケンス (SPI 値を用いる場合))



【図 25】

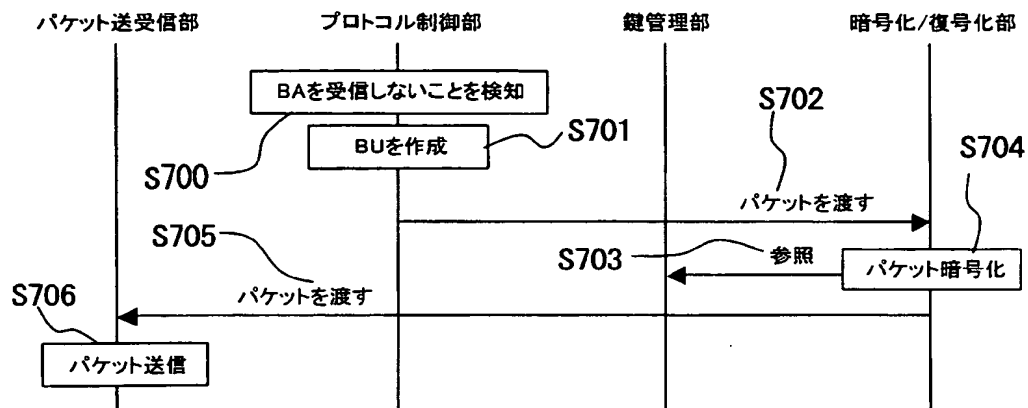
鍵受信装置 (MN) からの鍵再送要求メッセージにより、動的鍵 (共通鍵) を配する手順を説明するためのシーケンス図 (BU 再送時の鍵配布シーケンス (SPI 値を用いて再送 BU を判断する場合))



【図 26】

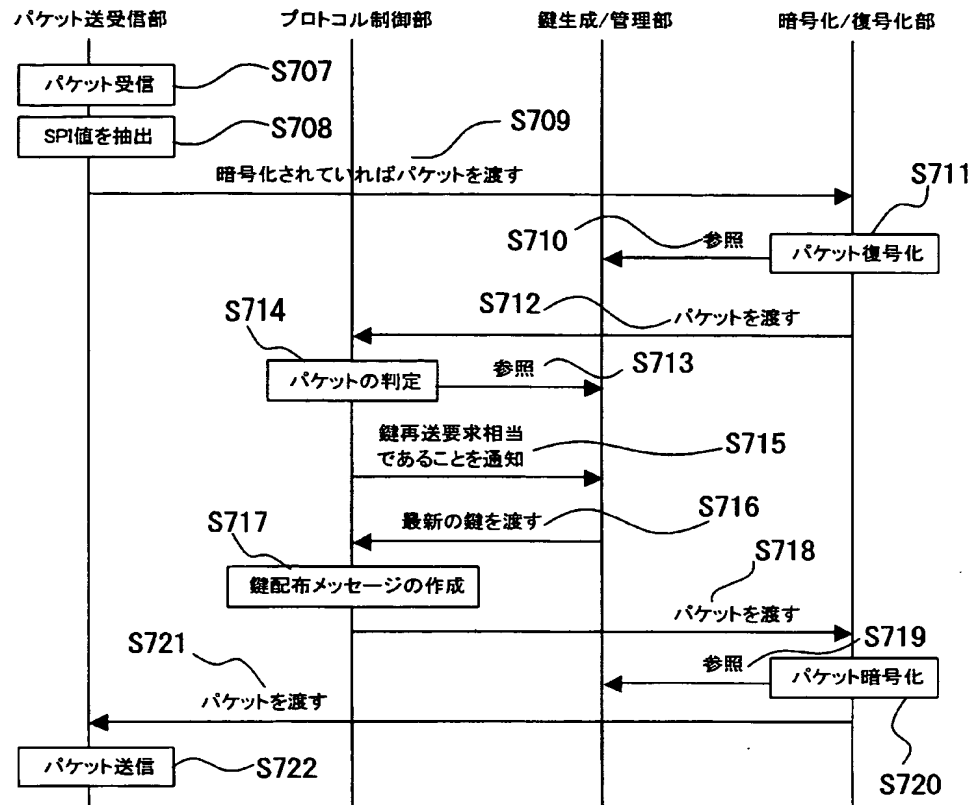
鍵受信装置 (MN) に着目したシーケンス図

( 鍵配布メッセージが破棄された場合の MN のシーケンス (SPI 値を用いる場合) )



【図 27】

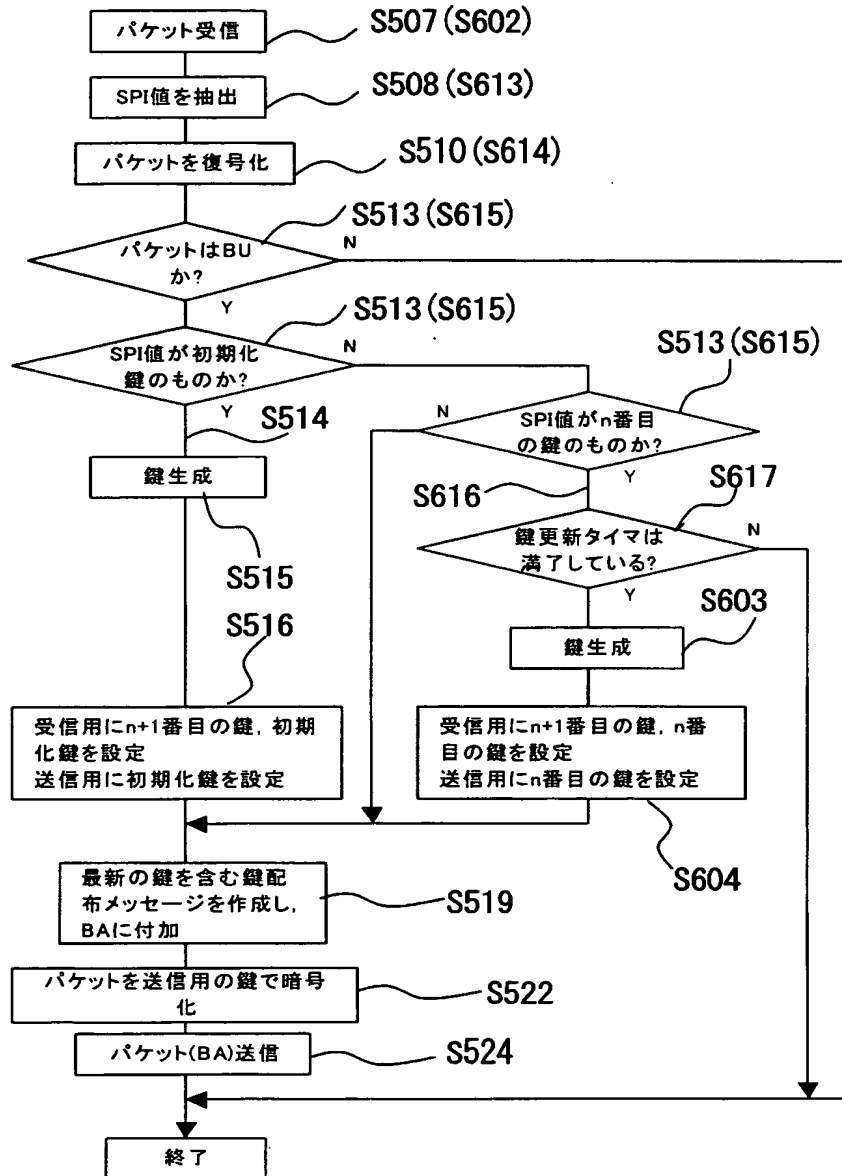
鍵送信装置（HA）に着目したシーケンス図  
(HA が鍵再送要求メッセージ相当の BU を受信した場合のシーケンス)



【図 28】

鍵送信装置 (HA) における概略処理を説明するためのフローチャート

(パケット受信時の鍵送信側装置 (HA) での処理フロー (SPI 値を用いる場合))



【書類名】 要約書

【要約】

【課題】 共通鍵暗号化通信を行う二つの装置の一方が他方に暗号化鍵を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も通信を継続する。

【解決手段】 鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第1保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第1設定手段と、を備え、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第2保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第2設定手段と、を備える。

【選択図】 図1



特願 2 0 0 2 - 3 4 8 7 4 8

出 願 人 履 歷 情 報

識別番号

[ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日  
[変更理由]

1 9 9 0 年 8 月 2 4 日  
新規登録

住 所  
氏 名

神奈川県川崎市中原区上小田中 1 0 1 5 番地  
富士通株式会社

2. 変更年月日  
[変更理由]

1 9 9 6 年 3 月 2 6 日  
住所変更

住 所  
氏 名

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号  
富士通株式会社